

## 보도자료

2011년 3월 6일(일) 배포 시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 네트워크정보보호팀 박철순 팀장 (☎750-2750)  
네트워크정보보호팀 이상국 사무관 (☎750-2757) sklee@kcc.go.kr

### 긴급 PC안전 수칙 발표 : “PC 켤때 안전모드 시작” - 새로운 명령이 추가된 악성코드 주의 요망 -

정부는 3월 6일(일) 악성코드가 명령서버로부터 두가지 새로운 명령을 다운로드 받도록 되어 있는 것이 발견되었다고 밝혔다. 새롭게 추가된 것은 감염된 좀비PC가 전용백신을 다운로드 받지 못하도록 보호나라([www.boho.or.kr](http://www.boho.or.kr)) 등 전용백신 사이트의 접속을 방해하는 기능과 하드디스크를 즉시 파괴하는 기능이다. 이번에 새롭게 밝혀진 것은 한국인터넷진흥원(KISA)이 안철수연구소가 확보한 악성코드 샘플을 공동으로 야간 작업을 통해 분석한 결과이다.

정부는 우선 KISA를 통해 악성코드에 감염된 좀비PC가 전용백신 사이트에 접속하지 못하게 될 경우에는 우회해서 접속할 수 있도록 조치하였다. 방통위는 악성코드에 감염되어 하드디스크가 즉시 파괴되는 피해를 최소화하기 위해 오늘 새벽 국가사이버안전센터(NCSC)로부터 악성코드 유포 및 명령 사이트로 추정되는 584개 IP를 확보하여 KISA와 ISP를 통해 긴급 차단하였다.(누적 차단 IP수는 총729개)

이제는 악성코드에 감염되면 백신치료도 쉽지 않고 하드디스크가 즉시 파괴될 수 있기 때문에 PC이용자는 우선 악성코드에 감염되지 않도록 주의해야 한다. 따라서 악성코드 유포지로 활용되는 정보공유 사이트에는 당분간 접속을 자제하는 것이 좋다. 정보공유사이트 관리자도 웹서버해킹 탐지도구인 휘슬(WHISTL - KISA에 요청)을 사용하여 악성코드를 탐지하고 삭제하는 것이 필요하다.

이번 하드디스크 파괴 증상은 명령서버로부터 명령을 받고 일정 기간이 지난 후에 동작했던 2009년 7.7 디도스때와는 달리, 명령을 받는 즉시 동작하도록 설정이 되어 있다. 하드디스크 파괴 명령이 하달되면 먼저 A~Z까지 모든 드라이브를 검색하여 zip, c, h, cpp, java, jsp, aspx, asp, php, rar, gho, alz, pst, eml, kwp, gul, hna, hwp, pdf, pptx, ppt, mdb, xlsx, xls, wri, wpx, wpd, docm, docx, doc 파일들을 복구할 수 없도록 손상시킨다. 그리고, A~Z까지 모든 고정 드라이브를 검색하여 시작부터 일정 크기만큼을 0으로 채워 하드디스크를 손상시켜 아예 컴퓨터 작동이 되지 않게 된다.

이에 따라 국민들은 꺼져있는 PC를 다시 켤 때는 반드시 안전모드로 부팅하여 디도스 전용백신을 다운로드받아 안전한 상태에서 PC를 사용해야 한다. PC 이용자는 다음과 같은 조치를 취하면 된다.

#### <긴급 PC 안전 부팅 수칙>

- 1) 네트워크 연결선(LAN선)을 뽑는다.
- 2) PC를 재시작한 후 F8을 눌러 (네트워크 가능한)안전모드를 선택하여 부팅한다.
- 3) 네트워크를 재연결한 후 보호나라([www.bohonara.or.kr](http://www.bohonara.or.kr)) 또는 안철수연구소([www.ahnlab.com](http://www.ahnlab.com))에 접속하여 디도스 전용백신 다운로드

※ PC가 이미 켜져 있는 경우에는 전용백신 곧 바로 다운로드

- 4) 디도스 전용백신으로 악성코드 치료후 PC 재부팅

아울러, 긴급 전용백신으로 치료가 완료되었더라도 변종 악성코드에 의한 공격으로 재감염될 수 있으므로 각별한 주의가 필요하다. 특히 국민들은 PC 사용시 백신 제품을 최신 엔진으로 업데이트하고 실시간 감시를 동작시켜 재차 감염되는 것을 방지해야 한다.

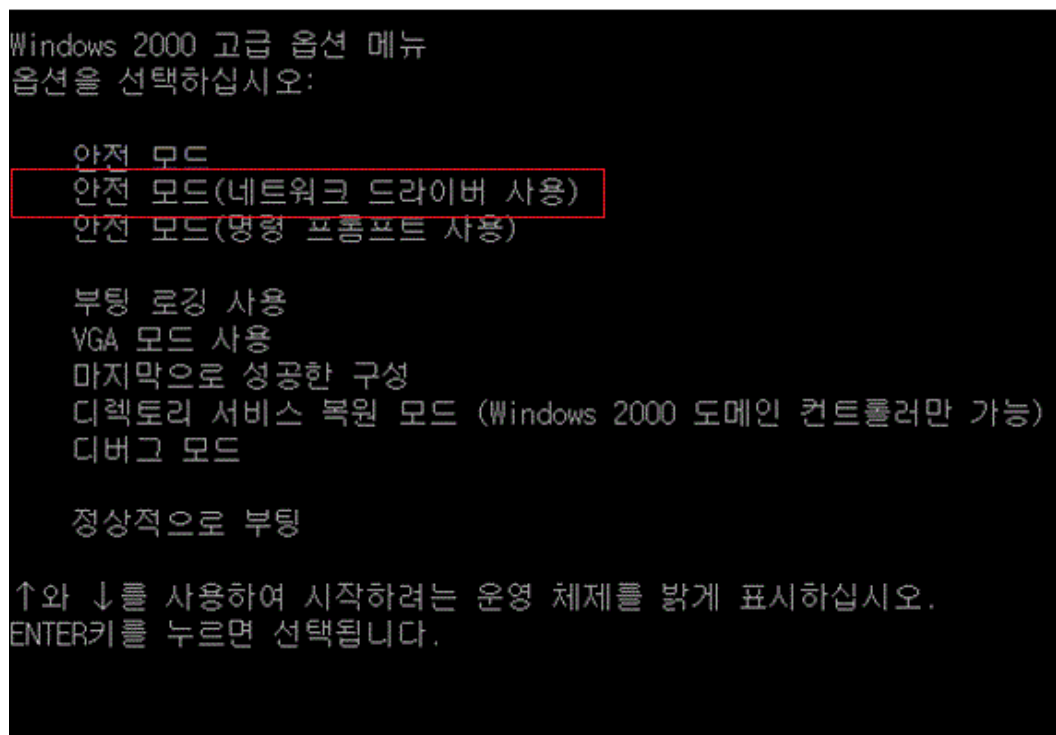
현재, 방송통신위원회, 국가정보원, 행정안전부, KISA, 안철수연구소 등으로 민관 합동의 공동대책반을 구성하여 금번 DDoS 공격에 신속하고 효율적으로 대응하고 있다.

## [안내] PC 안전수칙 상세 가이드

1. 네트워크 연결선(LAN선)을 뽑고 PC를 안전모드(네트워킹 사용)로 부팅.

안전모드 부팅하는 방법은 PC 부팅한 후 키를 연속적으로(0.5초 간격으로 탁!탁!탁! 누름) 누르시면 아래 그림과 같이 “화면으로 넘어가게 됩니다.

### A. 윈도 2000 의 경우 - 안전모드(네트워크 드라이버 사용) 선택



### B. 윈도 XP (Vista, Win 7, 2003, 2008 서버 공통)의 경우 - 안전모드(네트워킹 사용) 선택

Windows 고급 옵션 메뉴  
옵션을 선택하십시오:

안전 모드

안전 모드(네트워킹 사용)

안전 모드(명령 프롬프트 사용)

부팅 로깅 사용

VGA 모드 사용

마지막으로 성공한 구성 (작동한 최근 설정값)

디렉터리 서비스 복원 모드 (Windows 도메인 컨트롤러만 가능)

디버그 모드

시스템 오류 시 자동으로 다시 시작 안함

표준 모드로 Windows 시작

다시 부팅

위 아래 화살표를 사용하여 시작하려는 운영 체제로 이동하십시오.

## 2. 최신 전용백신 다운로드 및 실행

### A. 보호나라 홈페이지 (<http://www.bohonara.or.kr>) 접속

#### i. 메인 팝업창에서 '안철수연구소 전용백신 다운로드' 클릭

 보호나라 “보호나라에서 알려드립니다.”

**정부 및 금융기관 등 주요기관 홈페이지 DDoS 공격 발생에 따른 주의 경보 발령**

**□ 개 요**


- 3월 4일 국내 주요기관(기업)을 대상으로 DDoS 공격이 발생하고 있어 사이버위기 주의 단계 발령
- 악성코드를 치료하여 시스템 손상 등의 피해를 입지 않도록 주의

**□ 대응 방법**

- 인터넷 사용자는 전용 백신을 설치하여 악성코드 치료
  - 안철수 연구소 전용백신 다운로드**
  - 하우리 전용백신 다운로드**
- 악성코드 감염으로 인한 피해를 입지 않도록 MS 윈도우, 백신프로그램 등의 최신 보안업데이트 적용 유지
- 출처가 불분명한 이메일 및 불건전 홈페이지를 통한 감염 피해를 입지 않도록 주의

**□ 참 조**

- 관련정보 : [주의경보]
- 전화 : 국번없이 118



B. 안철수연구소 홈페이지(<http://www.ahnlab.com>) 접속

i. 메인 팝업창에서 '전용백신 다운로드 받기' 클릭



**Ahn** 안철수연구소

로그인 | 회원가입 | MY 보안

개인제품 | 기업제품 | 시큐리티 센터 | 보안정보 | 다운로드 | 고객지원

**안철수연구소 입니다.**

최근 국내 웹사이트를 겨냥한 DDoS 공격 및 시스템 손상을 일으키는 악성코드가 발견되었습니다. 이에 안철수연구소는 ASEC(시큐리티대응센터)과 CERT(컴퓨터침해사고대응센터)를 비롯해 전사 비상 대응 체제를 지속 가동하고 국가기관과 합동으로 적극적인 대응을 수행하는 한편 DDoS공격을 유발하는 악성코드에 대한 **전용백신**을 무료로 배포하고 있습니다.

DDoS 공격 예방 및 시스템 손상을 방지하기 위해 전용백신을 이용하여 검사를 권장드립니다. 추가로 V3 제품을 사용하시는 고객께서는 **최신 엔진 버전으로 진단 및 치료**할 수 있으며 새롭게 나오는 변형에 대해서도 예방이 가능합니다.

▶ **전용백신 다운로드 받기**

개인 및 기업 일반 사용자분들은 좀비 PC 방지는 물론 안전한 컴퓨터 이용을 위해서는 사용자 환경에 맞는 백신을 설치하여 반드시 최신 엔진 업데이트를 실행하여 주시기 바랍니다.

- 개인용 무료 백신 : **V3 Lite**
- 방화벽과 백신이 통합된 유료 보안 서비스 : **V3 365 클리닉**
- 기업용 통합 보안 : **V3 IS 8.0**

오늘 하루 항 열지 않기

3단계 : 주의

최신 엔진 업데이트 ▶  
2011.03.06.00

- \* [공지] 국내 40개 웹사이트 디도스 공격 경...
- \* [이벤트]V3 토크 이벤트 진행 중!!
- \* [이벤트]구매회원 중 총 123분께 푸짐한 선...
- \* [이벤트]축마고우를 찾습니다. 최대 90일 연...
- \* [공지] AhnLab V3 Zip 2.0 출시

**V3 365 클리닉**  
통합백신에서 웹보안까지, 토털 PC케어

**AhnLab Policy Center Appliance**  
보안관리와 비용절감을 위한 스마트한 3C

**DDoS 공격을 유발하는  
좀비 PC 예방법**

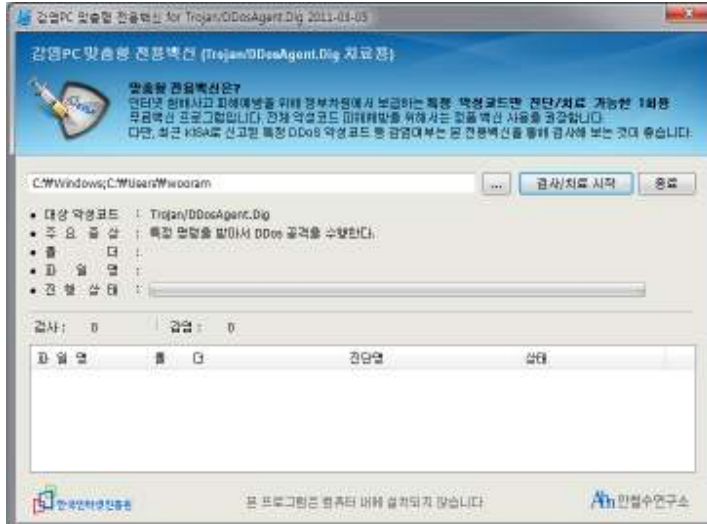
MORE ▶

트위터

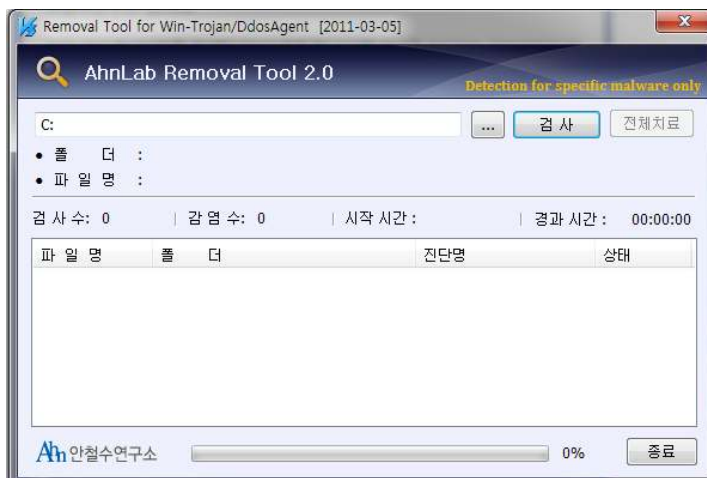
AhnLab\_man@blue2fly 헉 너무 급하게 내보내  
느라 알아채지 못했습니다 ㅠ

### 3. 전용백신 실행 후 '검사' 클릭

보호나라 홈페이지 안철수연구소 전용백신



안철수연구소 홈페이지 전용백신

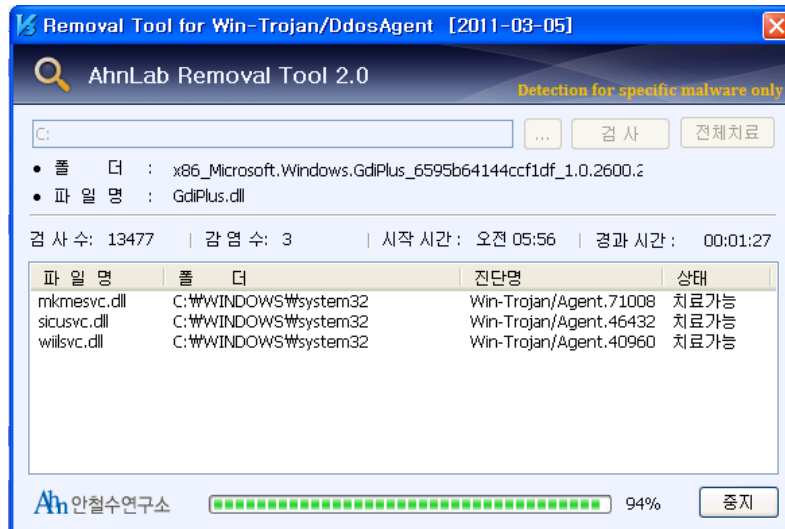




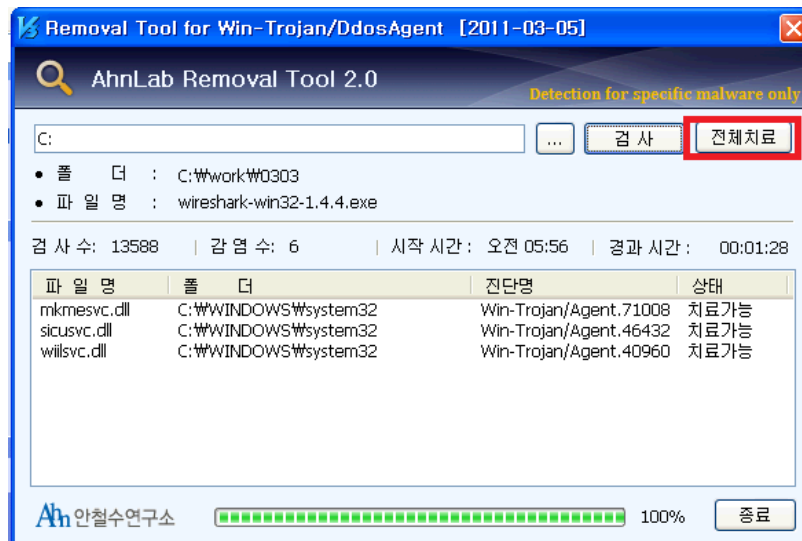


## B. 안철수연구소 홈페이지 전용백신

### i. 악성코드 발견

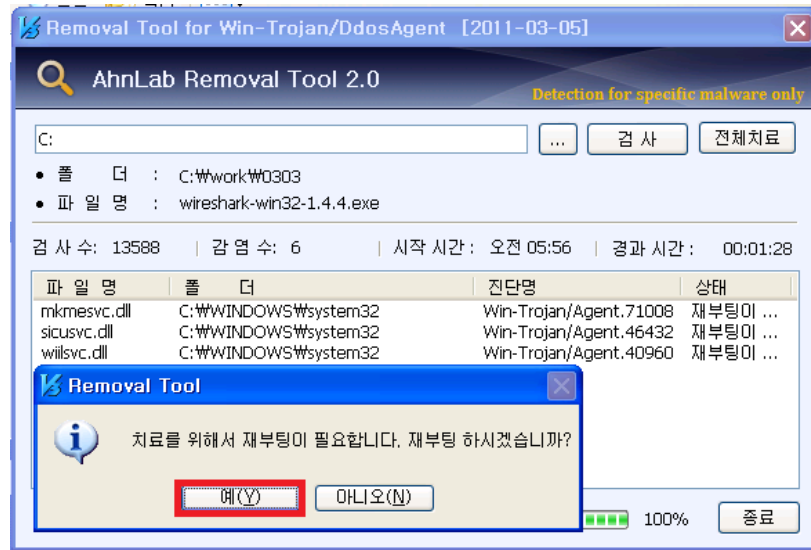


### ii. 전체치료 클릭





iii. '재부팅 하시겠습니까' 예(Y) 선택시 치료와 동시에 재부팅 진행



5. 검사 완료되면 '종료' 클릭 후 PC 재부팅