


www.hauri.co.kr

컴퓨터바이러스의 동향

Anti Virus Leader HAURI

권석철 ㈜하우리 대표이사
www.hauri.co.kr / scikwon@hauri.co.kr



Anti Virus Leader HAURI

컴퓨터 바이러스의 정의

협의의 의미
컴퓨터 시스템의 부트 영역, 메모리 영역, 파일 영역 중 어느 한 곳 이상에 감염되어 자기 증식 및 복제가 가능하고 특정한 환경 등에서 데이터 파괴성을 가지고 있는 악성 프로그램

광의의 의미
협의의 컴퓨터 바이러스 프로그램을 포함하여 시스템 침입, 데이터 유출, 파괴 등 시스템에 유해한 동작 유발을 목적으로 제작된 악성 프로그램을 총칭. (악성 코드)

Anti Virus Leader HAURI

컴퓨터 바이러스의 분류

감염부위별

- ✓ 부트바이러스 - 부트 섹터에 감염
- ✓ 파일바이러스 - 파일에 감염
- ✓ 산란형바이러스

악성코드 (광의의 바이러스)

- ✓ 백도어(Backdoor), 트랩도어(Trapdoor)
- ✓ 트로이 목마(Trojan Horse)
- ✓ 웜(Worm)
- ✓ 악성 스크립트(Malicious Script)
- ✓ Joke / Hoax

Anti Virus Leader HAURI

컴퓨터 바이러스의 분류

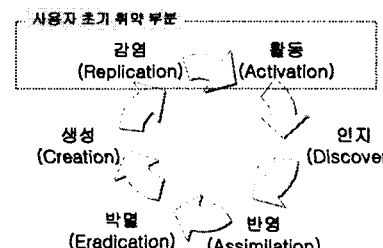
◆ 바이러스 명명(하우리)

I-Worm.Win32.Klez.H

Anti Virus Leader HAURI

컴퓨터 바이러스의 라이프사이클

사용자 초기 취약 부분



생성 (Creation) → 감염 (Replication) → 활동 (Activation) → 인지 (Discovery) → 반영 (Assimilation) → 박멸 (Eradication) → 생성 (Creation)

Anti Virus Leader HAURI

최근 바이러스의 동향

◆ 바이러스에 의한 피해유형

- 시스템 파괴
- 정보유출
- 연속적인 메일 송신등에 의한 시스템 과부하
- 정상적인 시스템 운영 불능
- 트래픽 증가로 인한 네트워크 마비
- 바이러스 벡터로 오인
- DDOS형 공격

최근 바이러스의 동향

◆ 해킹기술과 바이러스 기술의 통합화

출처: KISA

최근 바이러스의 동향

◆ 최근 등장한 바이러스의 특징

- 유입경로의 다양화**
: OS 및 S/W의 보안 취약점을 이용한 자동실행이나 네트워크를 통한 유입
- 네트워크 및 해킹 기술의 결합**
: 시종자 암호로 해킹 및 트로이목마 등 설치/실행
: 바이러스 기술과 결합한 DDOS 유행의 공격 시도 증가
- 피해의 대형화**
: 예전처럼 PC의 데이터를 파괴하는 지엽적인 피해에서 사회 전반적인 피해로 대항화 되는 추세임.
- 빠른 확산속도**
: 실시간에 전세계를 확산, 시차가 거의 없음.

최근 바이러스의 동향

◆ 최근 등장한 바이러스의 특징

- 보안 취약점 이용이 증가**
: 알려진 OS 및 각종 Application의 보안취약점이 다수 존재
: 보안의 취약점을 이용한 바이러스 제작 가능성도 증가
- 백도어 및 트로이목마 형 바이러스 증가**
: 정보의 유출, DDOS형의 공격 등의 피해 예상

↓

바이러스

최근 바이러스의 동향

◆ 주요 원의 피해 사례

- CodeRed Worm (2001. 7)**
 - 국내 피해 : 1만 7천 206개 기관에서 43378개 시스템
 - 대부분 기업체, 일반인 등 민간에서 집중적으로 발생
 - 피해기관 1476건, 방문기간 163건, 연구소 35건 [FIRST(국제침해사고대응협의회) 발표]
- Win32.Nimda (2001. 9)**
 - 전세계 100만대의 컴퓨터를 감염
 - 국내 피해 : 22000여건
 - 국내의 피해정황은 세계 4번째 [USA Today, 장봉복]

최근 바이러스의 동향

◆ 주요 원의 피해 사례

- Worm.SQLSlammer (2003. 1)**
 - 전 세계적으로 1월 25일 오후 4시 쯤에 출현된 후 사라지지 않은 MS-SQL 서버의 90%가 10분 이내의 감염
 - [CAIDA(Cooperative Association for Internet Data Analysis)보고]
 - 국내 피해 : 세계 감염시스템(약 7만 5천개)의 11.6%인 8300여대 세계에서 2번째
- Blastor (2003. 8)**
 - 2003년 8월 12일 MS사의 RPC 보안 취약점을 이용하여 감염
 - 전 세계적으로 20만 7천대의 시스템을 감염시킴(뉴욕-연방인포텍스).
 - 국내의 실제 감염건수 는 최소 100만대 이상으로 예상

최근 보그터 바이러스 분석

◆ 최근 바이러스 분석을 통한 특징

1999 2000 2001 2002

409-13-1 (13-13-14)권 **안티 바이러스 관련 기술**

<ul style="list-style-type: none"> - 취약점 분석 - 바이러스 시뮬레이터 - 네트워크 바이러스 방지 - 원격관리 	<ul style="list-style-type: none"> - 바이러스 분석 - 바이러스 진단/치료 - 바이러스 실시간 감시 - 메모리 치환 - Anti-Virus 자체 방벽 - 알리지자 같은 바이러스 방벽 	<ul style="list-style-type: none"> - 데이터 복구 - 시스템 설정 복원
--	---	---

409-13-1 (13-13-15)권 **하우리 전용백신 유료와 배경**

- 유료 고객과 무료 사용자가 동일한 서비스를 제공함으로써, 유료 고객들의 불만증가
- '백신=유료' 라는 인식을 근본적으로 바꿔, 유료 소프트웨어 사용자들에게 양질의 제품과 차별화 된 서비스 제공
- 정부의 백신 조달가 정상화 필요
- 직원 사기저하
- 주주 이익 분배라는 기업의 본질적 목적 고려
- 제품과 사후 지원서비스(A/S)에 대한 명확한 구분이 요함

409-13-1 (13-13-16)권 **하우리의 인재상**

- 일을 즐겁게 하는 인재
- 글로벌 마인드를 갖춘 인재
- 학력이나 기간 보다는 능력을 중시
- 조직에 동화되는 인재
- 현재 실력이 최고의 인재보다는 최선을 다해 최고가 되고자 하는 의지와 잠재력을 갖춘 인재

409-13-1 (13-13-17)권

Q & A

◆ 감사합니다.