10.4 웜

10장. 악성 소프트웨어

개요 (1)

- 웜은 자신을 복제하여 네트워크 연결을 통해서 컴퓨터에서 컴퓨터로 그 복제본을 전송
- 일단 한 컴퓨터에 도착하게 되면 웜은 복제를 시작하고 다시 확산시키기 시작
- 전자메일 바이러스는 시스템에서 시스템으로 자신을 확산시키기 때문에 웜(worm)의 성격을 어느 정도 가지고 있음
- 웜은 적극적으로 감염시킬 기계를 찾고, 감염된 기계는 다른 기계를 공격하기 위한 자동화된 출발기지로 사용됨

개요 (2)

- 시스템에서 시스템으로 확산하기 위해 네트워크 연결을 이용
- 시스템에서 작동하기 시작하면 바이러스, 트로이 목마, 그외 어떠한 방해나 파괴활동 가능
- 웜이 활용하는 네트워크 수단
  - 전자메일 설비(Electronic mail facility):
    - 자신의 복제를 다른 시스템에 메일로 전송
  - 원격 실행 능력(Remote execution capability):
    - 자신의 복제된 웜을 다른 시스템상에서 실행
  - 원격 로그인 능력(Remote login capability):
    - 웜은 원격 시스템에 로그인하고 한 시스템에서 다른 시스템으로 자신을 복사하는 명령 수행

개요 (3)

- 컴퓨터 바이러스와 동일한 특성
  - 잠복 단계, 확산 단계, 트리거 단계, 실행 단계
- 웜 확산단계
  1. 호스트 테이블이나 원격 시스템 주소의 저장소를 검사하여 감염시킬 다른 시스템을 탐색
  2. 원격 시스템과 연결을 설정
  3. 원격 시스템에 자신을 복사하고 그 원격 시스템 안에서 복사본을 구동
- 복사 이전에 감염 여부 확인
- 시스템 프로그램이나 다른 프로그램으로 위장

모리스 웜 (1)

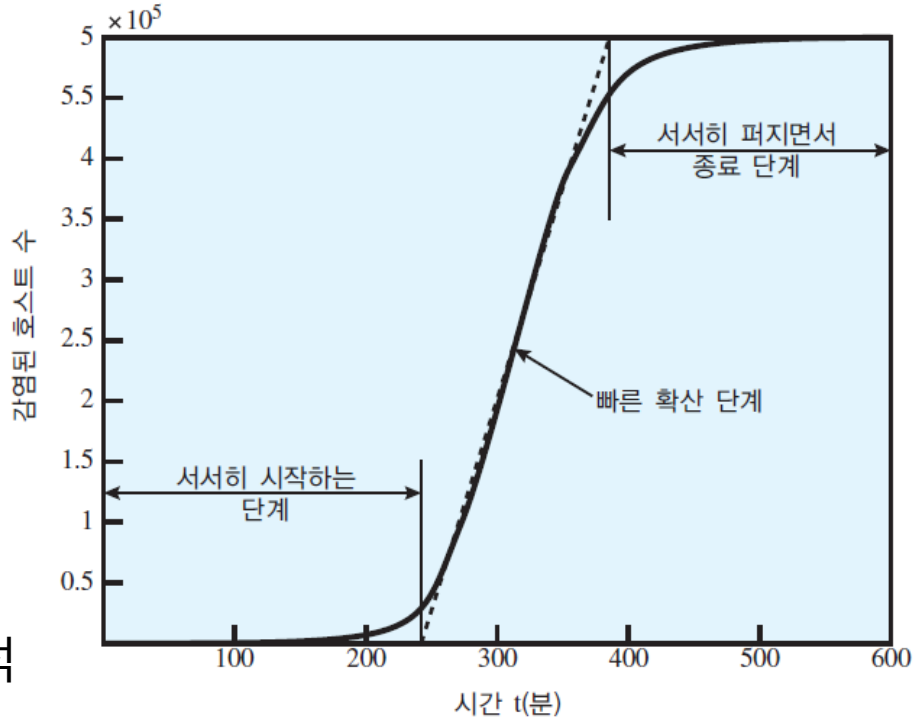
- 1998년 Robert Morris가 인터넷에 제공
- UNIX 시스템에서 퍼지도록 설계
- 확산을 위해 다양한 기술을 사용
  - 이 호스트에서 접근을 허용하는 다른 호스트 탐색 : 다양한 목록과 테이블 탐색
- 동작 원리
  1. 원격 호스트에 합법적 사용자로 로그온을 시도
     - 지역패스워드 파일을 크래킹하고 발견한 패스워드와 사용자 ID를 이용
  2. 패스워드 크래킹 프로그램은 다음을 수행
     - 각 사용자의 계좌 이름과 이들의 단순한 치환을 시도
     - 모리스가 생각했던 내장된 432개의 패스워드 목록을 시도
     - 지역 시스템 디렉터리에 있는 모든 단어를 시도

모리스 웜 (2)

- 동작 원리(계속)
  3. 원격 사용자 위치를 알려주는 finger 프로토콜 버그 이용
  4. 메일 송수신 원격 프로세스 디버그 옵션 안 트랩도어 이용
  5. 공격이 성공하면 웜이 쉘과 통신 가능
  6. 짧은 부트스트랩 프로그램 전송
  7. 프로그램 실행을 명령한 후 로그 오프
  8. 부트스트랩 프로그램에서 부모 프로그램을 호출하여 나머지 부분 다운로드

웜 확산 모델

- 확산 속도와 감염된 호스트 총 수에 영향을 주는 요인
  - 확산 모드
  - 이용되는 취약성
  - 이전 공격과의 유사성 정도
- 확산 3단계
  - 호스트수가 지수적으로 증가
  - 감염 속도가 줄어든다
    - 확산 증가는 거의 선형적
    - 감염 비율은 매우 높다
  - 공격 속도는 종료단계



최근의 웜 공격 (1)

- 코드 레드(Code Red) 웜
  - 2001년 7월 등장
  - 침투와 확산에 MS의 IIS(Internet Information Server)의 허점을 이용
  - 윈도우즈의 시스템 파일 검사기 기능을 마비
  - 다른 호스트로 확산시 랜덤 IP 주소 조사
  - 특정 기간 동안에는 확산만 수행
  - 특정 시점이 되면 특정 사이트를 대상으로 수많은 호스트가 엄청나게 많은 패킷을 전송해 처리를 못하도록 하는 서비스거부 공격을 개시
  - 활동을 중단하고 주기적으로 재활동
  - 두번째 공격에서 360,000개 서버 감염

최근의 웜 공격 (2)

- 코드 레드 II
  - 마이크로소프트 IIS를 타깃으로 한 변종
  - 희생 컴퓨터에 백도어(backdoor)를 설치해서 해커가 직접 행동할 수 있게 제작
- 2001년 후반 보다 다양한 기능을 가진 웜 등장
- 님다(Nimda)
  - 다양한 확산 메커니즘
    - 전자메일로 클라이언트에서 클라이언트로 확산
    - 개방 네트워크 공유를 통해 클라이언트에서 클라이언트로 확산
    - 침해당한 웹 사이트를 브라우징 하는 것으로 웹 서버에서 클라이언트로 확산
    - 적극적 스캐닝과 다양한 마이크로소프트 IIS 4.0/5.0 디렉터리 트래버설 취약점을 이용해서, 클라이언트에서 웹 서버로 확산
    - 코드레드 II 웜에 의해 남겨진 백도어를 찾는 것을 통해서, 클라이언트에서 웹 서버로 확산

최근의 웜 공격 (3)

- SQL 슬래머 웜(Slammer worm)
  - 2003년 초
  - MS SQL 서버의 버퍼 오버플로우 취약점을 이용
  - 극도로 축약되어 있으며 빠른 속도로 전파하여 10분 안에 90%의 취약한 시스템을 감염
- Sobig.f 웜
  - 2003년 말
  - 감염된 컴퓨터를 스팸 엔진으로 바꾸는 개방된 프록시 서버를 이용
  - 창궐했을 당시 모는 메시지의 1/17에 Sobig.f 포함, 24시간 내에 100만개 이상의 복제 전달

최근의 웜 공격 (4)

- 마이둠(Mydoom)
  - 2004년
  - 전자메일을 대량으로 전송하는 전자메일 웜
  - 감염된 컴퓨터에 백도어를 설치하여 해커가 신용카드 번호나 패스워드 같은 자료에 원격접속을 할 수 있도록 함
  - 1분에 1000번이 복제, 36시간 안에 1억개의 감염된 메시지 전파

최신 웜 기술의 특징 (1)

- Multiplatform:
  - 윈도우에 국한되지 않고, UNIX 계열의 다른 유형 플랫폼도 공격
- Multiexploit:
  - 다양한 방법으로 침투 시도
  - 웹 서버, 브라우저, 이메일, 파일 공유, 기타
- Ultrafast spreading:
  - 취약한 시스템의 인터넷 주소를 수집하기 위한 사전 스캐닝 수행
- Polymorphic:
  - 탐지되지 않고, 패스트 필터를 건너뛰고, 실시간 분석을 피하기 위한 바이러스의 폴리모픽 기술 이용

최신 웜 기술의 특징 (2)

- Metamorphic:
  - 자신의 외형 뿐만 아니라 매 확산단계에서 틀에 억매이지 않는 다양한 행동패턴을 나타냄
- Transport vehicles:
  - 순식간에 대량의 컴퓨터에 감염시킬 수 있으므로, 여러가지 분산 공격에 사용할 도구를 퍼뜨리는데 이상적
- Zero-day exploit:
  - 알려지지 않은 취약점을 교묘히 이용하여 웜이 확산된 다음에야 네트워크 공동체에 알려짐

이동전화 웜 (1)

- 2004년 처음 등장
  - 블루투스 연결이나 멀티미디어 메시지 서비스(MMS)를 통해 전파
- 웜의 목표
  - 스마트폰
- 모바일 전화 맬웨어
  - 전화기능을 완전히 마비
  - 전화기상의 데이터를 모두 삭제
  - 장치가 사용자 모르게 통신료가 비싼 서비스 제공 전화번호로 전화를 걸어 통신비를 과다하게 과금

이동전화 웜 (2)

- 컴워리어(CommWarrior)
  - 2005년
  - 블루투스를 이용해서 수신 가능한 영역에 있는 다른 전화기로 웜을 복제
  - 자신을 MMS 파일로 전화기 안의 저장된 전화번호로 전송하고 도착한 텍스트 메시지와 MMS 메시지에 대해 자동으로 응답하는 방식으로 자신을 복제
  - 자신을 탈착식 메모리 카드에 복제하고 전화기의 프로그램 설치 파일 안에 삽입

웜 대응책 (1)

- 바이러스에 대한 대응방법과 유사
- 안티바이러스를 통해 감지
- **네트워크 활동**이 증가하므로 이를 감시하여 방어
- 효과적인 웜 대응을 위한 필요 요소
  - 일반성(Generality):
    - 폴리모픽 웜을 포함한 다양한 웜 공격에 대처할 수 있어야
  - 적시성(Timeliness):
    - 초기에 대응하여 감염되는 수를 줄여야
  - 회복력(Resiliency):
    - 우회기법에 대해서도 대응할 수 있어야
  - 최소 DoS 비용(Minimal denial-of-service costs):
    - 방어 때문에 축소되는 기능과 서비스를 최소화해야
    - 정상적인 운용을 방해해서는 안됨
  - 투명성(Transparency):
    - 기존 OS, 소프트웨어 하드웨어를 수정해서는 안됨
  - 전역 및 지역적 방어(Global and local coverage):
    - 네트워크 외부와 내부 모두 방어할 수 있어야

웜 대응책 (2)

- 웜 대응책 6개 분류
  1. 시그너처-기반 웜 스캔 필터링(Signature-based worm scan filtering):
     - 웜 시그니처를 생성한 후 네트워크/호스트로 들어올 때 스캔하여 탐지
     - 폴리모픽 웜에는 한계
  2. 필터-기반 웜 억제(Filter-based worm containment):
     - A와 유사하나 웜 내용에 집중
     - 메시지를 점검하여 웜 코드가 들어있는지 확인
     - 예: 비지랜터(Vigilante) : 말단 호스트에서 협력적 웜 탐지기법 사용
     - 효과적인 탐지 알고리즘과 신속한 경보 발령 필요
  3. 페이로드-부류-기반 웜 억제(Payload-classification-based Worm Containment):
     - 패킷을 조사하여 웜이 포함되어 있는지 확인
     - 예: 네트워크에서 익스플로잇 코드 탐색

웜 대응책 (3)

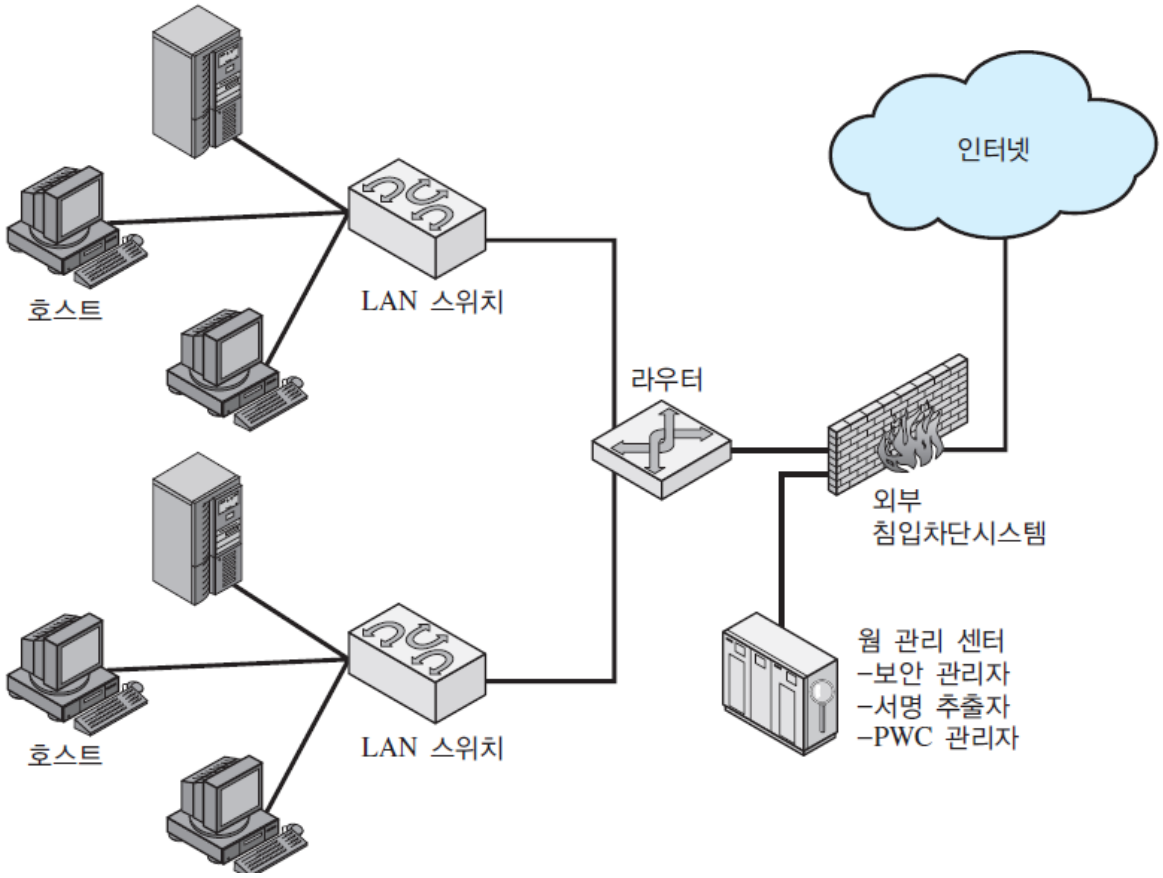
- 웜 대응책 6개 분류 (계속)
  4. 한계점 랜덤워크 스캔 탐지(Threshold random walk(TRW) scan detection):
     - 스캐너가 작동 중인지를 감지하는 수단
     - 스캐너가 무작위로 목적지를 선정하는 방법을 활용
  5. 속도 제한(Rate limiting)
     - 감염된 호스트에서 실행하는 스캔처럼 보이는 트래픽 속도 제한
       - 호스트가 윈도우 시간 안에 처음으로 연결할 수 있는 컴퓨터(IP 주소) 수 제한
       - 높은 연결 실패율 탐지
     - 정상적 트래픽도 지연시킬 가능성이 있음
     - 탐지를 피하기 위해 스스로 속도를 지연하는 스텔스 웜에는 무용
  6. 속도 정지(Rate halting):
     - 외부로의 연결 속도나 연결 시도의 개수의 한계점을 초과하면 즉각 차단
     - 실수로 막은 호스트를 신속하고 투명하게 풀어주는 방법을 갖추고 있어야 함

호스트 기반 웜 억제 (1)

- 호스트에 기반
  - 허니팟, 침입차단시스템, 네트워크 IDS 같은 네트워크 장비에 기반하지 않음
- 빠른 속도로 전파되는 웜 위협을 다루기 위해 설계
  - 밖으로 나가는 연결 시도의 빈도와 많은 원격 호스트로 연결을 시도하는 데 갑작스런 증가가 있는지 관찰
  - 갑작스런 증가가 발생되면 소프트웨어는 즉각 연결시도를 차단
- 관리자와 에이전트로 구성
  - 보안관리자, 시그니처 추출자, PWC 관리자가 단일 장치에 구현

호스트 기반 웜 억제 (2)

- 배치 예



호스트 기반 웜 억제 (3)

- 동작
  1. 에이전트는 나가는 트래픽을 모니터링해서 스캐닝을 하고 원격 호스트로 UDP나 TCP 연결 시도가 폭증하는지 아닌지를 결정
     - 갑작스런 증가 감지가 있으면 다음 행동
       - 로컬 시스템에 경보를 발령
       - 밖으로 나가는 모든 연결시도를 차단
       - 경보를 관리자에게 통보
       - D에서 설명하게 될 완화 분석을 시작
  2. 관리자는 경보 수령
     - 관리자는 경보를 모든 에이전트로 확산

호스트 기반 웜 억제 (4)

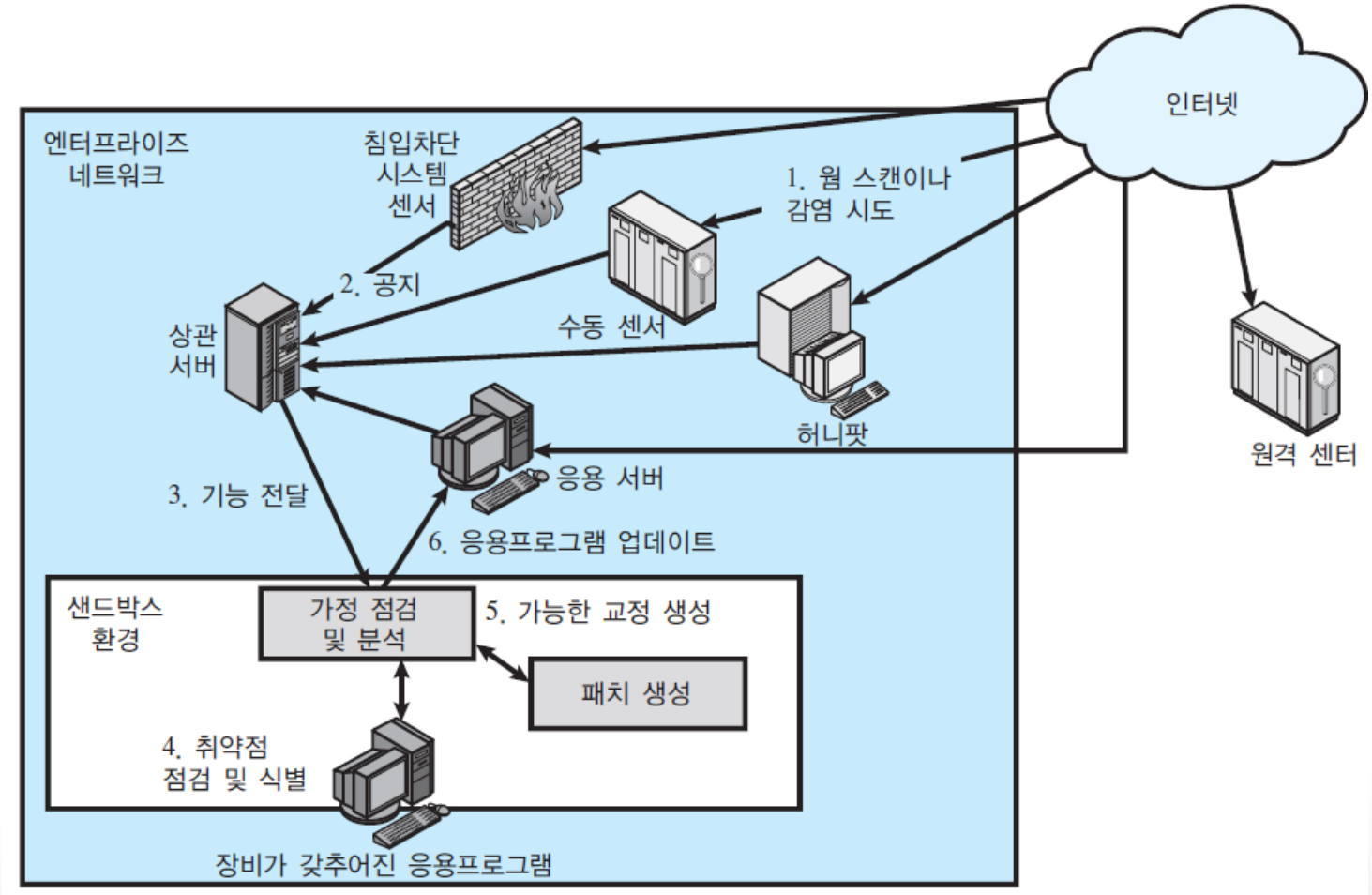
- 동작 (계속)
  3. 호스트는 경보를 수신
     - 에이전트는 경보를 무시할지 아닌지를 판단
       - 마지막으로 들어온 패킷 시간 이후로 충분한 시간이 지난 후 들어온 경보 : 무시
     - 그렇지 않은 경우 다음 조치
       - 특정 경보 포트에서 밖으로 나가는 모든 연결시도를 차단
       - 완화 분석을 시작
  4. 완화 분석
     - 에이전트는 밖으로 나가는 연결시도가 한계점을 넘었는지 아닌지 알아보기 위해 고정된 윈도우 시간 동안 밖으로 나가는 활동을 모니터링
       - 한계점 초과
         - 차단상태를 유지하면서 완화 분석을 또 다른 윈도우 시간만큼 시행
       - 밖으로 나가는 연결시도 수가 한계점 이하로 떨어져서 에이전트가 차단을 해제할 때까지 계속
       - 한계점을 초과하는 시간이 충분히 주어진 완화 분석 윈도우 시간을 넘어서면
         - 에이전트는 호스트를 분리하고 관리자에게 보고

네트워크-기반 웜 방어 (1)

- 웜 모니터링 소프트웨어
- 두 가지 유형
  - 진입 모니터(Ingress monitors):
    - 내부망과 외부망의 경계에 위치
    - 예: 사용되지 않는 IP로 들어오는 트래픽 관찰
  - 진출 모니터(Egress monitors):
    - 나가는 트래픽에서 스캐닝 흔적이나 기타 의심스런 행동 모니터링
- 침입탐지시스템의 기능처럼 작동하거나 중앙관리시스템에 경보 전달
- 제로-데이 익스플로잇(zero-day exploit)에 효과적으로 대응
  - 웜 공격에 실시간으로 반응하여 컴퓨터 보안 담당자가 알기 전에 컴퓨터 보안의 취약한 부분을 이용하는 대응시스템 구현 가능

네트워크-기반 웜 방어 (2)

- 웜 모니터 및 자동화된 패치시스템



네트워크-기반 웜 방어 (3)

- 동작
  1. 네트워크의 다양한 장소에 설치된 센서는 의심되는 웜을 탐지
     - 센서 논리를 IDS 센서에 내장
  2. 센서는 들어온 경보를 연관시키고 분석하는 중앙 서버로 경보를 전송
     - 연관 서버는 웜 공격이 관찰될 가능성과 웜 공격의 중요 특성을 판단
  3. 서버는 보안된 환경 안으로 이 정보를 전달
     - 웜으로 의심되는 대상을 보호된 영역인 샌드박스 안에서만 분석하고 테스트

네트워크-기반 웜 방어 (4)

- 동작 (계속)
  4. 보호된 시스템은 의심스런 소프트웨어에서 적절하게 계기화한 목표 응용프로그램 버전을 점검해서 취약점을 파악
  5. 보호된 시스템은 한 개 이상의 소프트웨어 패치를 생성하고 이를 테스트
  6. 만약 패치가 이 감염을 허용하지 않고 응용프로그램의 기능을 위태롭게 하지 않는다면, 시스템은 패치를 호스트로 보내어 목표로 한 응용 프로그램을 업데이트