행동기반 탐지를 우회하는 웜 자기방어 기법 제안

권오철 조재익 문종섭
고려대학교 정보경영공학전문대학원
{kwonoch chojaeik, jsmoon}@korea.ac.kr

Proposal of worm Self-Defense technologies avoiding Behavior-based detection

Ochul Kwon Jaeik Cho Jongsub Moon
Korea University Graduate School of Information Management & Security

요 약

초기의 웜은 감염 및 확산의 신속성을 중요시하였으나, 생존성은 고려하지 않았다. 하지만 보안도구(Anti-worm)의 발달에 따라 2004년 이후 대규모의 웜 확산에 의한 피해가 보고되지 않고 있다. 이에 웜도 보안도구를 회피하는 자기방어(Self-Defense) 기법을 개발하여 생존성을 증가시키면서 진화하고 있다. 본 논문은 현존하는 웜 자기방어 기법과 그 한계를 분석한 후 행동기반 탐지 기법을 우회하는 자기방어 기법을 제안하도록 하겠다.

Keyword : 웜, 자기방어, 탐지회피, 행동기반 탐지

1. 서 론

가장 최근에 발표된 대규모의 웜 피해는 2003 년 Slammer, Blaster 와 2004 년 Sasser 웜이었다[1,2,3]. Slammer 웜의 경우 10 분 만에 전 세계 90 퍼센트 이상의 취약 호스트를 감염시켜 금융, 교통, 공공기관에 걸쳐 장애를 유발시켰을 정도로 강력한 웜이었다. 2003 년 1 월 25 일 국내 ISP 업체의 DNS 서버를 마비시켜 인터넷 대란을 발생시킨 웜이기도 하다. 그 후 정보보호의 중요성이 부각되고, 보안도구(Anti-worm)의 발달과 보안 정책 강화, 시스템관리자들의 보안의식이 강화됨에 따라 위와 같은 대규모의 웜 피해는 보고되지 않았다.

웜 제작자들도 이런 보안여건을 고려하여 웜을 제작하기 시작하였다. 대규모 확산 방식의 웜은 보안장비에 의해 탐지되고 차단될 확률이 높으므로 위험이 적고 느리게 전파되는 웜이 유행하였다. 또한, 프로세스, 레지스트리 은폐뿐만 아니라 보안 제품의 방어기법을 우회하는 자기방어(Self-defense) 기술을 사용하는 웜이 증가하였다[4].

즉, 빠른 전파능력뿐 아니라 웜의 생존성을 보장할 만한 기능이 고려되어 제작되었다. 초기의 회피 기술은 보안도구의 패턴 검색을 회피하기 위해 일부 코드를 수정하는 변종 제작이 주였으나, 점차 기술이 발달하여 Anti-worm 프로그램을 중지시켜 작동하지 못하게 하는 수준까지 진화하였다.

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다. (2007-SW-51-DM-01)

하지만 웜 분석가들도 이러한 우회 공격 기술을 차단하는 기법을 연구하였고, 대다수의 우회 공격이 탐지 가능하게 되었다[7,9,10,11].

본 논문은 웜의 보안도구 우회 기법들의 동향과 그 한계점을 분석하고 행동기반 탐지를 우회할 수 있는 자기방어 기법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 웜의 자기방어에 대한 관련연구를 살펴보고, 3 장에서는 기존 탐지기법을 우회할 수 있는 자기방어 기법을 제안한다. 마지막으로 4 장에서는 결론 및 향후 연구에 대해 설명한다.

2. 관련 연구

본 장에서는 침입탐지기법을 소개하고 보안도구를 침입탐지를 우회하는 공격방법에 대한 기존 연구를 알아보고 우회공격의 한계점을 분석하도록 하겠다.

2.1 침입탐지 기법 소개

침입탐지 기법은 크게 지식기반(Knowledge-based) 탐지와 행동기반(Behavior-based) 탐지가 있다. 지식기반 탐지는 기존 공격에서 얻은 공격 단서를 바탕으로 공격을 탐지하는 기법으로, 오용탐지(misuse detection)라고 불리기도 한다. 행동기반 탐지는 시스템이나 사용자의 정상행위를 지속적으로 관찰한 후 정상행위를 벗어나는 행동을 탐지하는 기법으로 비정상행위(anomaly detection) 탐지라고 불리기도 한다[8].

지식기반 탐지는 웜 탐지 확률이 높은 장점이 있으나, 이미 알려진 웜에 대해서만 탐지가 가능하다는 단점이 있다. 행동기반 탐지의 경우 알려지지 않은 웜 공격을 미리 발견하여 차단할 수 있는 장점이 있으나, 오탐율이

상대적으로 높다는 단점이 있다[6].

현재 각 연구소 및 대학에서 연구되고 있는 행동기반 탐지 기법은 다음과 같다[6].

2.1.1 TRW(MIT)

MIT에서 이루어지고 있는 수학적인 알고리즘인 (Threshold Random Walk)[12] 방법을 이용해서 트래픽 패턴을 분석하여 웜을 찾아내는 방법이다. 이 방식은 TCP 프로토콜에서 SYN 패킷을 스캐닝 동작으로 보고 연결의 성공 실패에 따라 스캐닝 공격여부를 판단하는 기법이다.

2.1.2 DEWP (ISI)

DEWP(Detecting Early Worm Propagation through Packet Matching)[13] 방식은 ISI(Information Sciences Institute)에서 제안한 방식으로, 네트워크 상에 유입되는 트래픽들을 특정 패턴들로 분류하여 웜을 탐지하는 방식이다. 이 방식은 특정 서비스 포트로 유입되는 트래픽의 양이 많게 될 경우 웜 트래픽으로 판단하는 방식이다.

2.1.3 Statistical Intrusion Detection 방식 (University of Massachusetts, Amherst)

SID[14]는 통계학적인 방식으로 웜을 탐지하는 방식으로 실제 전염병 같은 것의 전파를 설명할 때 쓰이는 Epidemic Model을 사용한다. CodeRed와 Slammer웜에 대한 자료를 수집하여 실제 웜의 모델을 만들고 실제 트래픽과 모델의 일치성을 확인하여 탐지하는 방식이다.

2.1.4 Autograph Project (CMU)

Autograph Project[15]는 Carnegie Mellon University에서 수행되고 있는 프로젝트로 웜으로 추측되는 패킷들을 수집하여 자동으로 웜에 대한 시그너쳐(signature)를 생성하는 방식이다. 공통 패턴을 찾는 방법은 Rabin's Fingerprint[16]방식을 사용하게 된다. 이 알고리즘은 간단한 모듈러 연산을 이용해 공통부분을 찾게 되는데 실제 구현이 쉽고 동작이 빠르므로 많은 곳에서 활용되고 있다.

2.2 침입탐지를 우회하는 자기방어 기법

최근 가장 많이 사용되는 악성코드의 자기방어 기법은 <표 1>과 같이 분류된다[5]. 표에서 보는 바와 같이 지식기반 탐지를 우회하는 기법과 보안도구에 대한 공격 기법이 주로 사용되고 있다.

<표 1> 웜 자기방어 기법

우회 유형	세부 기법
코드 수정 (Source modification)	다형성(Polymorphism)
	난독성(obfuscation)
	암호화(encryption)
실행 압축	Packing
시스템 은닉	Rootkit
보안도구 대항 (Combating antivirus)	보안도구 중지
	Host 파일수정으로 update 차단
	바이러스 파일로의 접근 제한

2.3 웜의 자기방어 기법의 한계

보안도구 우회 기법을 이용하는 웜의 증가에 따라 우회기법을 탐지하는 기술도 발달하였다.

코드수정 기법은 일반 실행코드에서 자주 사용되지만 다형성 웜에서는 사용될 수 없는 검증명령어의 분포를 비교하여 다형성 웜을 판단하는 방법으로 탐지가 가능하다[7].

실행압축 기법은 프로세스가 실행되는 순간부터 API 추적을 시작하여 각각의 프로세스마다 프로세스의 상세정보와 접근 자원정보, API 호출 순서를 저장하여 이를 정형화된 악성코드와 유사성을 비교하는 방법으로 탐지가 가능하다[9].

Rootkit은 Rootkit이 주로 변조하는 시스템 명령을 정형화한 후 시스템에서 발생되는 변조 명령의 증가를 원격 감시 서버로 모니터링 하는 것으로 탐지가 가능하다[10].

보안도구 대항은 보안도구들의 작동상태를 통제하는 ESM(Enterprise Security Management System) 구성으로 각 보안도구의 작동상태 감시를 통해 공격을 탐지할 수 있다[11].

3. 웜 자기방어 모델 제안

본 장에서는 행동기반 비정상 탐지 기법을 우회할 수 있는 웜 자기방어 모델을 제안하도록 하겠다.

3.1 스캔방식 변형

TWR 방식과 DEWP 방식의 경우 웜의 특성 중 Target Discovery 단계[17]에서 대상 호스트를 스캐닝하는 행위를 근거로 탐지하는 방식이다. 두 연구의 기본 가정은 탐지하고자 하는 웜이 CodeRed웜과 Slammer웜과 같이 취약 호스트를 랜덤 스캔한다는 것이다. 랜덤 스캔을 할 경우 연결의 실패율이 증가하고 네트워크 트래픽이 증가함을 이용한 방식이라 하겠다. 하지만 기존 웜의 스캔유형을 따르지 않는 스캔의 경우 이러한 탐지방법을 우회할 수 있다.

가능한 스캔방식으로는 host information-based scan이 있다. 이 방식은 감염 호스트의 host파일을

읽거나 네트워크 트래픽을 감청하여 연결가능한 IP 테이블을 작성한 후 취약 호스트를 스캔하는 방식이다. 랜덤 스캔에 비해 정확도가 높고 감염대상이 적으므로 연결 실패를 최소화하고 트래픽 증가도 최소화 할 수 있다. 또한, 기존에 사용되던 연결과 유사한 형태를 보이므로 이상 트래픽을 보이지 않는 장점이 있다.

3.2 확산방식 변형

SID방식의 경우 발견된 웜을 모델링하여 새로운 웜의 형태와 비교하는 방식으로 새로운 웜이 기존 웜과 유사한 확산방식을 따를 것이라고 가정하는 탐지 방식이다. 따라서 모델링된 확산유형을 따르지 않는 웜의 경우 탐지 우회가 가능하다.

가능한 확산 방식으로는 Random delay propagation이 있다. 확산간에 랜덤한 대기시간을 추가하거나 네트워크 트래픽의 유동량을 고려하여 시간대별 확산 간격을 달리함으로써 기존 모델과 다른 확산유형의 웜 제작이 가능하다.

그림 1은 2004 년 10 월 28 일부터 11 월 4 일경까지 국외에서 국내로 유입되는 트래픽 전체를 수집한 것을 일단위로 시간당 패킷양으로 나타낸 그래프이다[18].

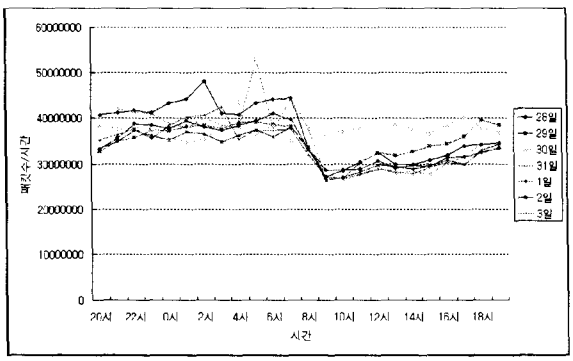

그림 1. 국외에서 국내로 유입되는 트래픽 양 (Packets/Hour)

그림 1을 통해 오전시간대와 저녁시간대의 패킷 유동량이 다른 것을 알 수 있다. 따라서 저녁시간에는 짧은 대기시간으로 확산하고 오전시간에는 긴 대기시간으로 확산할 경우 이상 트래픽 증가를 이용한 탐지 회피가 가능하다.

3.3 가변적 Payload 사용

Autograph방식은 이상 트래픽에서 웜의 특정한 패턴을 추출하고자 하는 방식이다. 하지만 모듈러 연산을 기본으로 하므로 웜의 payload 순서를 치환하고 임의의 데이터를 삽입하여 길이를 변경할 경우 탐지 회피가 가능하다.

행동기반 탐지 우회 방법을 <표 2>와 같이 정리할 수 있다.

<표 2> 행동기반 탐지를 우회하는 자기방어 모델

우회 유형	세부 기법
스캔방식 변형	모델링 되지 않은 방식으로 취약 호스트 스캔
확산방식 변형	확산 모델링 임계치 이하로 확산 속도 조절
가변적 Payload	Payload의 순서 치환 및 길이 변경

4. 결론 및 향후 연구

본 논문에서는 최근 웜의 보안도구 탐지를 우회하는 자기방어 기법과 그 한계를 소개하고 행동기반 탐지 기법을 우회하는 웜 자기방어 모델을 제안하였다.

웜 제작자는 악성코드 분석가가 어느 수준까지 분석할 수 있을지를 알 수 있을 정도로 웜을 분석한다[7]. 그리고 방어를 위해 보안도구가 사용할 기법들도 연구한다. 그만큼 웜의 생존성을 보장하기 위해 연구하는 것이다. 따라서 보안도구 제작자는 시스템의 취약성을 지속적으로 패치하듯이 보안도구의 취약점을 지속적으로 개선하여 방어기법을 회피하는 사례를 최소화하도록 하여야 하겠다.

향후 연구로는 웜의 우회기법 사용 패턴을 분석하여 자동화된 탐지를 가능하도록 하는 연구가 있다.

참고 문헌

[1] David Moore, et al., "Inside the slammer worm," IEEE Magazine of Security and Privacy, pp. 33-39, July/Aug. 2003.

[2] Symantec. w32.blaster.worm. http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.wor%m.html, 2003.

[3] Symantec. w32.sasser.worm. http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm%.html, 2004.

[4] 안철수연구소, "악성코드 동향 및 대응방안", 제 2 회 국방 정보보호체계 발전 세미나, 2007.

[5] Kaspersky, "The evolution of self-defense technologies in malware", http:// www.viruslist.com /en/analysis?pubid=204791949, 2007.

[6] 신승원, "인터넷 웜 공격 탐지 방법 동향", 전자통신동향분석 제20권 제1호, pp. 9-16, Feb, 2005.

[7] H Debar, "Towards a taxonomy of intrusion-detection systems", Computer Networks Vol. 31, pp. 805-822, 1999.

[8] 이기훈, "다형성 엔진으로 생성된 웜의 탐지기법", 2006년도 한국정보과학회 가을 학술대회발표 논문집, Vol. 33, No. 2(C), pp. 515-520, 2006.

[9] 박남열, "우회기법을 이용하는 악성코드 행위기반

탐지 방법", 정보보호학회논문지, Vol. 16, No. 3, June. 2006.
[10] 김지영, "보안침해사고 대응을 위한 커널 루트킷 탐지 시스템 설계", 한국인터넷정보학회 학술발표대회 논문집, Vol 6, No. 1, pp 45-48, 2005.
[11] 이창우, "분산 환경에서의 침입방지를 위한 통합보안 관리 시스템 설계", 한국컴퓨터정보학회 논문지, Vol. 11, No. 2, pp. 75-82, 2006.
[12] J.Y. Jung, S. Schechter, and Arthur W. Berger, "Fast Detection of Scanning Worm Infections," RAID 2004, Sophia Antipolis French, Sep. 2004.
[13] Xuan Chen and John Heidemann, Detecting Early Worm Propagation through Packet Matching, Technical Report ISI-TR-2004-585, 2004.
[14] Cliff Changchun Zou, Weibo Gong, and Don Towsly, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," ACM WORMS '03, Washington DC, USA, Oct. 2003.
[15] H.A. Kim and Karp Brad, "Autograph: Toward Automated, Distributed Worm Signature Detection," 13th USENIX Security Symposium, Aug. 2004.
[16] Bro NIDS, http://www.bro-ids.org/
[17] Weaver N., "A taxonomy of computer worms", Proceeding of the 2003 ACM workshop on Rapid Malcode, pp 11-18, Oct. 2003.
[18] 김정형, "마이닝을 이용한 이상트래픽 탐지: 사례 분석을 통한 접근", 정보과학회 : 정보통신, Vol. 33, No. 3, pp 201-217, 2006.