국방정보통신망에서 사이버공격에 대비한 악성코드 감염 예방에 관한 연구

김성환*, 박민우*, 엄정호**, 정태명***
*성균관대학교 전자전기컴퓨터공학과
**대전대학교
***성균관대학교 정보통신공학부
e-mail:shkim47@imtl.skku.ac.kr

A Study on Prevention against Malware Infection defending the Threat of Cyberwarfare in Defense Network

Sung-Hwan Kim*, Min-Woo Park*, Jung-Ho Eom**, Tai-Myoung Chung***
*Dept of Electrical and Computer Engineering, Sungkyunkwan University
**Daejeon University
***School of Information Communication Engineering, Sungkyunkwan University

요 약

2011년 Stuxnet의 출현을 기점으로 사이버공격이 보다 정밀화·구체화 되고 있으며 사이버전의 주요 무기라 할 수 있는 악성코드들의 특정 국가산업·기관시스템에 대한 직접적이고 지속적인 공격 시도가 예상된다. 본 논문에서는 사이버전의 개념, 악성코드 관련 동향과 공격행위별 감염대상 등을 살펴보고, 국방정보통신망에서 사이버공격에 대비한 악성코드 감염 예방방안을 제안한다.

1. 서론

2011년에 출현한 스턱스넷(Stuxnet)은 기존의 사이버 공격과는 달리 특정 목표를 선택하여 정밀하게 공격하는 차별화된 악성코드(Malware)로서 최근 여러 관련기관에서 이에 대한 분석과 대응방안이 활발히 논의되고 있다[1].

이전의 웜(WORM) 바이러스가 대상 네트워크에 부담이나 혼란을 가하는 Side Effect 위주의 방법을 사용한 반면에 스턱스넷은 보편적인 컴퓨터 환경이 아닌 대규모 생산공정 감시제어시스템인 SCADA(Supervisory Control And Data Acquisition)와 같은 국가산업·기관의 중요 시설을 직접 통제하여 2차, 3차적인 피해를 유도하는, 보다 직접적인 공격방법을 사용하고 있다. 이는 사이버공간에서 일어나는 새로운 형태의 전쟁인 사이버전에 즉시 사용가능한 주요 사이버 정밀공격무기로 평가받고 있다[2,3].

사이버전에서 사이버무기라고도 정의할 수 있는 악성코드에 대한 대응책도 현재 활발히 논의되고 있는데 이에 대한 대응책을 국방 분야에도 적극 적용하여 적의 사이버 공격으로부터 아군의 정보통신체계를 안전하게 보호하여야 할 것이다. 이러한 사이버전의 중요성을 인식하여 국방부는 2010년에 '국군 사이버사령부'를 창설하여 사이버전 수행능력 강화에 중점을 두고 있다[4].

본 논문에서는 사이버공격과 악성코드의 정의, 동향 및 공격행위에 따른 감염대상을 살펴보고 국방망 PC에 바로 적용 가능한 악성코드감염 예방방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 사이버전과 사이버 공격에 대해 살펴보고 3장에서는 악성코드의 정의와 국·내외 동향, 감염대상별 공격행위를 정리한다. 4장에서는 국방망 PC에 적용 가능한 취약요소별 악성코드감염 예방방안을 제안하고 5장에서 결론을 맺는다.

2. 사이버전의 개념

2.1 사이버전과 사이버 공격

국방부는 사이버전(Cyberwarfare)을 "사이버 공간에서 일어나는 새로운 형태의 전쟁수단으로서, 컴퓨터시스템 및 데이터 통신망 등을 교란, 마비 및 무력화함으로써 적의 사이버체계를 파괴하고 아군의 사이버 체계를 보호하는 것"으로 정의하였다[5,6].

사이버 공격은 컴퓨터와 네트워크를 기반으로 시스템과 전자장비 등으로 구성된 사이버 공간에서 악성코드, 웜·바이러스, 논리폭탄, EMP 폭탄 등의 사이버 무기체계를 이용하여 공격대상 시스템을 마비 파괴하거나 저장된 정보의 변경·유출 등의 사고를 유발하는 행위를 말한다[3,7].

이러한 사이버 공격은 공격대상에 적용되는 기술방식에 따라 소프트웨어 방식과 하드웨어 방식으로 구분 할 수 있는데 소프트웨어 공격은 해킹이나 논리폭탄, 인터넷 웜, 바이러스, 스팸메일 등과 같이 시스템이나 네트워크의 취약점을 이용하여 시스템 내의 자원을 탈취 및 파괴하거나 이를 원격제어 하여 다른 공격에 사용하는 공격을 말하고, 하드웨어 공격은 칩핑(Chipping)이나 나노머신, 전자기파 폭탄(EMP Bomb) 등을 사용하여 목표체계의 물리적 기능

을 제한 또는 파괴시키는 공격을 말한다[3].

2.2 사이버 공격의 최근 양상

최근 네트워크 환경의 발전과 IT산업 발전에 따라 사이버 공격의 형태도 지능화, 정밀화, 대량화 되어 가고 있다.

이전의 공격들은 대체로 업무 메일로 위장하여 악성코드를 전파하였으나 최근에는 SNS, 광고 배너, 웹하드 등을 통해 다양화되고 지능화된 경로로 공격을 시도하고 있다. 스턱스넷처럼 대형 기간시설의 특정시스템을 목표로 하는 정밀공격이 나타나고 있으며, '11년 3.4 DDoS 공격과 같이 십만 여대의 좀비 PC가 동원되는 대규모된 공격 양상을 보이고 있다[3].

3. 악성코드

3.1 악성코드 정의 및 현황

악성코드는 "Malware"라고도 하며 이는 악성 소프트웨어 "Malicious Software"의 줄임말로 악의적인 목적을 가지고 제작되어 컴퓨터에 악영향을 끼치는 모든 소프트웨어를 칭한다. 국내에서는 "Malware"를 "악성코드"로 총칭하고 있다[8]. 컴퓨터 기술의 발전과 인터넷 사용의 급증에 따라 수많은 악성코드들이 출현하였으며 이에 대한 변종들도 기하급수적으로 증가하고 있다. 컴퓨터 바이러스(Virus), 웜(Worm), 트로이목마(Trojan Horse), 스파이웨어(Spyware), 루트킷(Rootkit)등이 모두 악성코드에 속한다. 악성코드는 전 세계적으로 매년 증가하고 있는데, 안철수 연구소에서 조사한 1986년 이후 누적 악성코드 추정치는 2011년 기준 '1억 7700만'에 달한다. 이는 2010년에 비해 약 21% 증가한 수치이다.

3.2 악성코드 동향

2011년 악성코드 통계분석보고서에서 한국인터넷 진흥원과 안철수 연구소가 발표한 2011년 국내악성코드 침해사고의 주요 동향을 살펴보면 과금을 유발하거나 온라인 뱅킹정보를 노리는 모바일관련 악성코드와 국내 주요 행사 및 기관, 대형기업을 노리는 지능형 공격(APT:Advanced Persistence Threat)의 폭발적 증가, 윈도우 취약점의 악용에 대하여 공통적으로 언급하고 있다. 이는 악성코드 공격이 모바일 분야로 확대되고 있으며, 공격대상도 직접적이고 구체적으로 변화하고 있고, 가장 많은 사용자를 가지고 있는 윈도우 운영체제의 취약점에 대해 지속적인 공격이 발생하고 있음을 알려준다. 특히 스턱스넷 출현 이후 듀큐(Duqu)와 같은 변종이 등장하고, 주요 기업과 기관에 대한 지능화된 공격이 증가하고 있는 현상을 통해 국내 국방망에 대한 적극 방어의 중요성이 계속 증대 되고 있다[9].

3.3 악성코드 공격행위

인터넷의 질적, 양적 확대와 네트워크 인프라의 복잡도 증가에 따라 악성코드의 공격방법 또한 매우 다양해 졌다. [11]에서는 악성코드의 공격을 감염경로, 실행주체, 공격대상, 공격행위별로 구분하고 이를 구체화하였다.

다음 4장에서는 위의 구분 중에서 감염대상별 공격행위에 초점을 두고 국방망 PC에 적용한 악성코드감염 예방방안을 제안한다.

<표 1> 악성코드 감염대상별 공격행위[11]

구분	감염대상	공격행위
감염대상별 공격행위	네트워크	정보유출
		서버 접속
		대량 트래픽 전송
		가로채기
		전송지연
		스팸
	시스템	강제 시스템 제어
		자원 관리
		네트워크 설정 변경
		시스템 설정 변경
		디스플레이 설정 변경
	파일 시스템	파일생성
		파일파괴
		파일변조
	프로세스	제어
		모니터링
	입출력장치 오작동	미디어 제어
		입력장치 제어
		출력장치 제어
		기타 장치 제어

4. 국방망 PC의 악성코드 감염예방 방안

4.1 국방망 정의 및 특성

국방망은 다양한 종류의 호스트와 네트워크로 구성된 대규모 분산 네트워크 환경이지만 외부와는 분리된 폐쇄망이며 물리적으로는 여러 개의 도메인으로 구성되지만 논리적으로는 일종의 단일망으로 볼 수 있다[12].

국방망은 시스템관리자의 단위시스템 통제가 일반망보다 훨씬 엄격하고 구체화 되어 있기 때문에 효과적인 정책과 지침에 대한 학습 및 기대효과가 매우 높다고 할 수 있다.

4.2 국방망 PC 악성코드감염 예방방안

앞서 언급한 바와 같이 국방망은 외부의 인터넷과는 분리되어 있는 폐쇄망 이지만 기타 외부매체를 통한 감염위험을 완전히 배제할 수는 없다.

3장에서 살펴본 악성코드의 공격행위에 대응하기위해 공격행위 감염대상을 중심으로 국방망 PC 악성코드감염 예방방안을 다음과 같이 제안한다.

4.2.1 네트워크 분야

국방망 네트워크는 폐쇄형 이기 때문에 외부의 네트워크 공격에는 대응하기가 쉬운 장점이 있으나 반대로 내부에서 네트워크 이외의 이동매체를 통해 악성코드 공격을 받았을 경우 민첩한 대응을 하지 않으면 그 피해가 매우

커질 수 있는 단점이 있다. 서론에서도 언급한 스턱스넷 같은 악성코드는 네트워크 구성정보를 탈취하여 이를 공격에 사용하기 때문에 네트워크 접근경로와 구성정보를 암호화 하여 관리하여야 하고 네트워크 관리자가 악성코드 실행을 탐지하였을 때 Trigger 형태의 자동대응 절차를 수립하여 피해복구 및 내부 확산차단을 동시에 수행하여야 하겠다.

4.2.2 운영체제 취약점 보완

한국인터넷진흥원의 '11년도 해킹사고에 대한 운영체제별 분류를 살펴보면 윈도우 운영체제에 대한 피해가 7,731건(66%)으로 단연 높다. 이는 그만큼 많은 사용자가 윈도우 운영체제를 사용한다고 볼 수 있으며 그에 따라 윈도우 운영체제를 대상으로 한 악성코드도 많이 발생하고 있는 것으로 판단할 수 있다. 국방망도 가장 많이 사용하고 있는 윈도우 운영체제의 악성코드 감염 예방을 위해 다음과 같은 윈도우 시스템 취약점에 대한 예방책을 국방망에 적용해야 하겠다[10].

■ IIS(Internet Information Services) 취약성

IIS는 MS社의 윈도우 NT용 인터넷 서버 소프트웨어이다. IIS는 웹서버, FTP 서버, SMTP 서버 등 여러 서버의 기능을 통합하고 있으며 IIS를 이용하는 사용자들은 MS社의 프론트페이지(FrontPage) 제품을 사용하여 웹페이지를 만들 수 있다. 또한 사용자들은 ASP 기술을 이용할 수 있는데, 이것은 웹페이지 내에 액티브 X를 내장한 응용 프로그램들이 포함될 수 있다는 것을 의미한다. 공격자는 윈도우 NT용 인터넷 서버 서비스를 제공하는 IIS의 보안 취약성을 이용하여 악성코드를 감염시킬 수 있다. 서버라는 특징상 특정한 서비스를 사용자에게 제공하기 위해 서비스 관련 포트를 계속 열어놓게 되는데 이러한 취약성을 이용하여 외부에서 쉽게 내부로 침투할 수 있으며 웹서버가 감염되면 해당 서버에 접속하는 사용자들도 쉽게 악성코드에 감염되는 취약점이 있다. 이에 대한 예방책으로 IIS와 함께 설치되는 기본서비스를 재검토하여 필요치 않은 서비스(FTP 등)의 사용과 익명 계정 로그인 접속을 금지하여야 한다. 또한 원격코드 실행(Remote Procedure Call)을 금지하여 외부의 원격제어를 차단하여야 한다[11,13].

■ 윈도우 시스템 취약 : 레지스트리

레지스트리는 윈도우의 모든 설정을 담고 있는 중앙 저장소라 할 수 있다. 윈도우 시스템은 레지스트리를 통해 시스템에 대한 중앙 집중화와 각 사용자에 대한 설정과 권한을 관리한다. 따라서 악성코드들은 윈도우 시스템의 레지스트리를 추가하거나 변조하여 악성코드를 정상코드인 것처럼 실행시킨다. 이를 예방하기 위해 국방망에 사용하는 PC의 레지스트리 수정 및 추가에 대한 권한을 관리자나 슈퍼관리자에게만 부여하여 레지스트리 접근을 제어하여야 한다[11].

4.2.3 파일 및 프로세스 제어

악성코드 유형 중 '11년 기준으로 가장 높은 비율을 차지하는 악성코드는 트로이 목마(Trojan Horse)이다. 이 악성코드는 자신의 실체를 드러내지 않으면서 마치 다른 프로그램의 한 유형인 것처럼 가장하여 활동하는 프로그램이다. 트로이 목마는 자기 복제를 하지 않으며 다른 파일을 감염시키거나 변경시키지 않는다. 하지만 이 악성코드를 실행하는 순간, 시스템은 공격자에게 시스템을 통제할 수 있는 권한을 부여하게 된다[9,11].

이에 대한 예방책은 파일관리와 밀접한 관련이 있다. 확장자가 'EXE' 등과 같은 각종 실행파일들에 대한 자동실행 기능을 차단하고 반드시 백신 등의 검증 Tool을 통해 확인하여 식별되지 않은 실행파일을 철저히 감시하여야 한다. 또한 부주의나 기타 다른 사유로 악성프로그램이나 프로세스를 실행하였을 경우 추가피해 방지를 위한 프로그램·프로세스 강제 종료 Tool을 PC 내에 설치하여야 할 것이다.

4.2.4 입출력장치 제어

국방부는 전군을 대상으로 USB를 이용하지 않고 내부 전산망과 외부전산망 사이에서 자료를 교환할 수 있는 서버를 구축 중에 있다[14] 이는 그간의 USB관련 보안사고를 원천적으로 봉쇄할 수 있다는 점에서 대단히 높이 평가할 수 있다. 그러나 정보통신기술의 발전과 함께 스마트폰이나 클라우드컴퓨팅 같은 새로운 개념의 입출력 장비가 출현하고 있기 때문에 이에 대한 대응 또한 계속해 나가야 할 것이다. 스마트폰의 경우 모바일 관련 악성코드가 해마다 급증하고 있으며 앱(App)에 대한 보안 검증 체계가 없는 안드로이드 마켓의 개방성을 악용한 악성코드의 유포사례가 증가하고 있는 추세로 단말기를 통해 PC를 감염시키는 'Cardtrap.A' 같은 악성코드가 국방망을 공격할 수 없도록 군내 스마트폰 반입 시 아래 그림과 같이 별도의 국방악성코드 차단 앱을 설치하여 모바일 악성코드의 감염을 예방하여야 하겠다[9,10].

(그림 1) 모바일 악성행위 차단 방안

4.2.5 White-list 기반 프로그램 제어

'Daonol' 이란 악성코드는 어도비(Adobe)제품의 취약점

을 이용한 악성코드로, 허위 PDF 파일을 만들어 악성코드에 감염시킨다. 감염된 PC는 검은 화면에 마우스만 나타나는 부팅장애를 일으킨다. 이처럼 우리가 흔히 아는 어도비나 안티바이러스 프로그램을 가장한 가짜 프로그램을 통해서도 악성코드에 감염될 수 있다[11].

이에 대한 보완책으로 국방망 PC에 프로그램 설치 시 시스템관리 부서에서 검증하고 승인한 프로그램만 설치하여 사용자의 부주의나 임의적 판단으로 인한 검증되지 않은 프로그램의 사용을 차단하여야 한다.

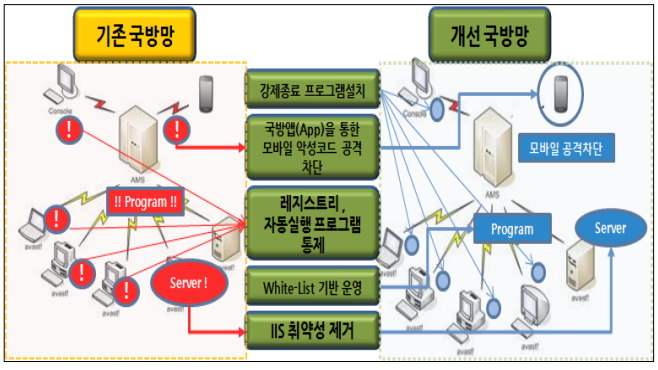
이는 화이트- 리스트 기반 프로그램제어라 할 수 있는데 화이트리스트(White-list)란 사용가능(허용된)한 목록으로서, 제한 및 금지의 개념이 포함된 블랙리스트(Black-list)와는 반대 개념이다. 국방망에서 PC를 관리 및 통제함에 있어 수없이 생겨나는 악성코드의 변종을 일일이 대응하는 것 보다는 검증 한 후 사용가능한 프로그램에 대해서만 철저히 통제하고 관리함으로써 악성코드를 효과적으로 예방할 수 있을 것이다[13].

4.3 맞춤형 국방망 PC 운영환경 조성

서론에서 언급한 스턱스넷과 같이 정밀하고 지능적이며 시간의 흐름에 따라 수없이 많은 변종이 생겨나고 있는 악성코드의 사이버 공격에 대응하기 위해서는 民·官·軍의 유기적인 협력을 통한 공동 대응이 필요하다.

주요 협력의제로 악성코드 분석정보 및 치료 방안 공유, 악성코드 조기경보체계 공동구축 등이 가능할 것이다[15].

이를 위해 국방 사이버전을 책임지는 국군 사이버사령부는 정부 산하 국가 전산망 침해사고 주관기관인 한국인터넷진흥원(KISA)과 같은 국가 주요기관과 안철수 연구소와 같은 국내 주요 보안 벤더(Vendor)들과의 협력체계를 구축하여 최신의 사이버 공격 기술정보를 공유하고 이에 대한 대비책을 세워야 하겠다. 또한 국방망에 설치하고자 하는 각종 운영체제나 소프트웨어 구매 시 생산업체와의 사전협약을 통해 상용 판매용 버전(Version)이 아닌 본 논문에서 제안한 악성코드 예방방안 등을 포함하고 군의 요구조건을 반영한 맞춤용 소프트웨어를 도입하여 운용함으로써 사용자의 참여를 통한 예방이 아닌 시스템적으로 근본적인 악성코드 감염예방을 추진할 수 있을 것이다.



(그림 2) 국방망 운영환경 개선안

5. 결론

본 논문은 국방망을 대상으로 사이버공격에 대비하기 위한 악성코드감염 예방방안을 제시하였다. 사이버공격의 여러 종류 중 소프트웨어 무기체계로 분류되는 악성코드 공격의 방어에 중점을 두고 공격행위별 감염대상을 구분하여 각각의 취약점 중 국방망에 적용 가능한 악성코드감염 예방방안을 제안하였다. 아울러 민관군의 협력을 통한 사이버 공격 공동대응 방안과 국방망 운영환경 개선을 통한 효과적인 악성코드 예방방안을 제안하였다.

ACKNOWLEDGEMENT

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 중점연구소 지원사업으로 수행된 연구임 (2011-0018397).

참고문헌

[1] Thomas M. Chen, "Stuxnet, the Real Start of Cyber Warfare?", IEEE Network, Nov/Dec 2010.

[2] Ralph Langner, "Stuxnet : Dissecting a Cyberwarfare Weapon", IEEE Security and Privacy, Vol.9 No.3, pp.49-51, May/June 2011.

[3] 엄정호 외 2명, "사이버전 개론", 홍릉과학출판사, 2012.

[4] YTN 기사, "군 사이버사령부 오는 11일 창설", 2010. 1. 8.

[5] 남길현, "군의 사이버전 대응체계 현재와 미래", 정보과학회지, 제23권 제7호, 2005.

[6] 엄정호 외 3명, "사이버 공격과 보안기술", 홍릉과학출판사, 2009.

[7] James A. Lewis, " Cyberwar Thresholds and Effects", IEEE Security and Privacy, pp23-29, Sep./Oct. 2011.

[8] G/McGraw and G. Morrisett. Attacking malicious Code:A Report to the Infosec Research Council. IEEE Software,17(5):33-41, Sept./Oct. 2000.

[9] 안철수 연구소, "2011년 악성코드 통계 분석 보고서", 2012.

[10] 한국인터넷진흥원, "인터넷 침해사고 동향 및 분석월보", 2011 vol.12, 2011.

[11] 한국인터넷진흥원, "악성코드 유사 및 변종 유형 예측방법 연구", 2011.

[12] 장희진 외4명, "국방망에서 세션분석기반의 침입자 역추적 시스템", 한국컴퓨터종합학술대회 논문집, Vol. 33, No. 1(C), 2006.

[13] 허재준 외 1명, "스턱스넷(Stuxnet)의 감염 경로와 대응방안", 정보보호학회지, 제21권 제7호, 2011.

[14] 아시아 경제 기사, "군 '저장장치 USB' 사용금지령", 2011. 4. 13.

[15] 엄정호 외 2명, "사이버전 위협에 대비한 전사적 조기경보체계 구축 방안", 한국정보처리학회 추계학술대회 논문집, 제17권 2호, 2010.