중소기업 환경에서 악성코드 유형 분석과 대응 방안

홍준석* · 김영희* · 박원형** · 국광호***

요 약

현재 각종 PC 및 정보시스템의 발전으로 인하여 인터넷이 급속도로 확산되고 있으며 이러한 인터넷 사용 증가에 따른 악성코드의 위협이 심각하게 나타나고 있다. 특히 보안인력 및 투자가 부족한 중소기업은 중요서버 및 내부 PC 대상으로 악성코드에 감염되었더라도 확인 및 조치가 불가능한 실정이다. 중소기업에서 실시하고 있는 중앙 집중형 방식의 보안관제형 악성코드탐지서비스를 분석하고 대응방안을 제시한다.

Analysis and Countermeasure of Malicious Code in Small Businesses

Jun Suk Hong* · Young hee Kim* · Won Hyung Park** · Kwang Ho Kook***

ABSTRACT

Due to the development of various information systems and PC, usage of Internet has rapidly increaced which lead to malicious codes rapidly spreading throughout the Internet. By the increasing use of the Internet, the threat by malicious codes has become a serious problem. In particular, Small businesses which lack investments in security personnels makes it impossible to verify and measure the servers and PC infected with malicious codes. We have analized malware infection types by using malicious code detection technology of security monitoring service and proposed countermeasures in small businesses.

Key words : Malware, Small Businesses, network security, network monitoring

접수일(2015년 12월 2일) 게재확정일(2015년 12월 18일)

* 서울과학기술대학교 IT정책대학원/산업정보시스템 전공
** 극동대학교 사이버보안학과
*** 서울과학기술대학교 기술경영융합대학/글로벌융합산업공학과(교신저자)

1. 서 론

현재 각종 PC 및 정보시스템의 발전으로 인하여 인터넷이 급속도로 확산되고 있다. ITU에 따르면 2013년의 세계 인터넷 이용자 수는 27억 1,000만명이며[1], 한국인터넷진흥원이 실시한 인터넷이용 실태조사에 따르면 우리나라 인터넷 이용자 수는 4,008만명(전년대비 196만명 증가)으로 나타났고 이 수치는 우리나라 전체국민의 82.1%가 인터넷을 이용하고 있는 것으로 나타났다[2].

이처럼 인터넷 사용이 급격히 증가함으로써 다양한 형태의 사이버 위협들이 나타나고 있다. 그 중에서 악성코드는 빠른 속도로 진화하고 있으며, 이제는 단순하게 악성코드 유포가 실력과시 목적이 아닌 금전적 정치적 군사적인 목적을 가지고 일어나고 있다.[3]

보안인력 및 투자가 부족한 중소기업은 중요서버 및 내부 PC가 악성코드에 감염되었더라도 확인 및 조치가 불가능한 실정이다[4]. 또한 중소기업은 안티바이러스만 설치해 놓고 실시간 감시 기능 활성화, 지속적인 업데이트, 정기적인 검사 등 기본적인 관리활동이 미비한 상황이다. 본 연구는 중소기업의 2,500개 PC에 설치된 악성코드 탐지 시스템으로부터 발생한 1년간의 악성코드 탐지유형을 분석하고 중소기업기술지킴센터에서 실시하고 있는 악성코드탐지체계 및 향후 발전방향을 제시하는 것이다. 본 연구의 범위는 악성코드유형과 분석, 중소기업기술지킴센터에서 탐지된 악성코드 감염현황 분석, 동 센터의 탐지 및 대응 그리고 향후 발전방안을 제시하는 것이다. 본 연구를 통해 안티바이러스를 이용한 중소기업의 적합한 악성코드 대응방안을 제시 할 수 있을 것으로 기대된다.

2. 관련 연구

2.1 악성코드 분류 및 특징분석

악성코드는 악의적인 목적으로 개발되어 시스템 운영을 방해하고 사용자에게 피해를 입히는 소프트웨어이다. 사용자의 허가 없이 시스템에 침투하거나 설치되어 자원오남용, 정보탈취, 서비스거부공격 등의 악성 행위를 행하는 프로그램이다[5]. 이러한 악성코드는 사용자에게 다양한 피해를 입힐 수 있는 특징을 가지고 있으며 일반적으로 컴퓨터바이러스(computer virus), 웜(worm), 조크, 트로이목마(trojan horse), 스파이웨어(spyware)으로 분류할 수 있다.

2.1.1 컴퓨터바이러스(computer virus)

정상적인 파일이나 부트 영역에 사용자 몰래 자신의 코드를 삽입하거나 감염시켜 활동하는 프로그램으로 시스템을 파괴하거나 작업을 방해하며 다른 파일에 기생한다[6].

2.1.2 웜(worm)

자기 복제성을 가진 프로그램으로 독립적으로 존재하며 시스템을 감염시켜 사용자가 해당 프로그램을 실행하지 않아도 스스로 실행되며 PC에 존재하는 취약점을 찾아 네트워크를 통해 전파되어 다른 시스템을 감염시킨다[6].

2.1.3 조크(joke)

악의적인 목적 없이 사용자의 동요나 불안을 조장하는 가짜 컴퓨터 바이러스 또는 프로그램으로 물질적인 피해는 없다[6].

2.1.4 트로이목마(trojan horse)

정상적인 프로그램으로 위장하여 사용자가 해당 프로그램을 실행하도록 만든 후에 중요 자료 삭제, 정보 탈취 등을 목적으로 이용되는 프로그램으로 바이러스와 달리 시스템 파일을 감염시키지 않는다[6].

2.1.5 스파이웨어(spyware)

광고의 목적보다는 사용자의 인터넷 접속 정보 등을 수집하기 위해서 제작된 소프트웨어를 의미한다. 애드웨어와 혼용되어 사용되지만, 스파이웨어는 애드웨어와 다르게 사용자의 개인정보 등을 외부로 유출시키는 특징을 갖는다[6].

2.1.6 악성코드 종류별 특징

다음 <표1>는 악성코드 분류에 따라 다음과 같은 특성을 비교하였다[7].

<표 1> 악성코드 종류별 특징 분석

구분	주요 목적	감염 대상	자기 복제	존재 형태	대책
바이러스	데이터손실(삭제, 손상)	파일/부트	O	기생, 독립	치료
웜	급속확산	X	O	독립	삭제, 차단
트로이목마	데이터 손실, 정보유출	X	X	독립	삭제
스파이웨어	사용불편, 불안	X	X	독립	삭제
혹스/조크	심리적 거부, 불안	X	X	독립	삭제, 무시

악성코드 별 특성을 보면 바이러스를 제외한 나머지 악성코드들은 파일의 형태가 독립적이므로 치료를 위해서는 해당 파일을 삭제 및 원복하면 된다. 바이러스는 정상 파일을 대상으로 변조하므로 치료를 위해서는 복원 또는 복구를 해야 한다.

트로이목마는 정보유출을 목적으로 하며 웜의 경우에는 시스템 자원을 손상시키기 위한 목적으로 사용이 된다. 스파이웨어 및 혹스/조크는 사용자 불편 및 심리적 불안을 유발시킬 목적으로 이용이 되어 진다.

2.2 기존 악성코드 대응 기술

악성코드 대응 방법으로는 첫 번째, 안티바이러스를 이용하여 방화벽 및 실시간 기능 활성화를 통해 기존에 알려져 있는 악성코드에 감염 되는 것을 방지하는 것이다. 두 번째, 샌드박스(SandBox)를 이용하는 것이다. 샌드박스는 PC에 다운로드 되는 파일을 샌드박스에서 실행해 본 후 이상 유무를 파악 후 이상이 없는 경우에만 다운로드가 실행되게 하는 방법이다[8]. 세 번째는 악성코드 분석과 지속적인 모니터링을 통해 악성코드 감염을 최소화해 나가는 것이다. 24시간 모니터링을 통해 다양한 로그, 패킷을 수집하고 이 수집된 데이터를 분석하여 분석된 내용을 바탕으로 보안을 강화 해 나간다면 PC 및 시스템, 네트워크 등 다양한 취약점에 의해 악성코드에 감염 되는 것을 최소화 할 수 있다.

3. 중소기업 악성코드 감염 유형과 대응 문제점

해마다 악성코드는 증가하고 있으며 이러한 악성코드에 감염된 PC는 좀비PC화 되어 DDoS 공격에 악용되거나, 중요한 자료 및 개인정보의 유출 등 악의적인 행위로 인해 피해를 입고 있다. 특히 대기업에 비해 중소기업은 악성코드의 감염여부에 대해서 인지도 못하고 있으며 또한 악성코드의 감염여부를 확인하였다고 할지라도 조치방법에 대해 몰라서 조치가 어려운 경우가 있다. 이러한 중소기업의 악성코드 감염에 대해 한국산업기술보호협회의 중소기업기술지킴센터는 중소기업청의 지원으로 중소기업에 악성코드 탐지 프로그램을 배포하여 악성코드에 감염 시 통보 및 조치를 지원하고 있다.

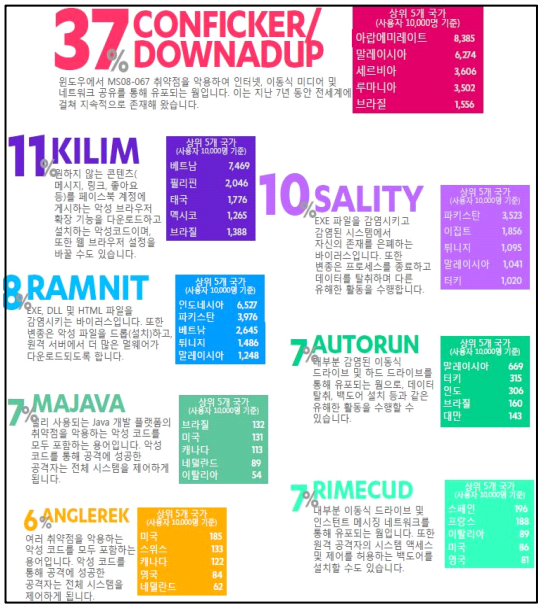
3.1 악성코드 감염 유형 분석

2014년 악성코드 중 가장 큰 특징은 첫째, PC상의 중요폴더 및 하드디스크를 암호화하여 암호화 해제 비용을 요구하는 랜섬웨어의 지속적 증가이다. 2014년에는 cryptolocker와 같은 기존의 보안 위협에 유포 방식, 암호화 및 결제 방식을 한층 더 업그레이드 함으로써 진화는 계속되고 있다.

둘째, 취약점을 악용한 악성코드가 지속적으로 증가하고 있다. 이는 OS와 애플리케이션의 패치가 적용 되지 않고 있다는 것을 나타낸다. exploit kit 같은 악성코드는 악의적인 목적으로 제작된 웹사이트에 툴킷을 숨겨 이곳에 방문하는 사용자들의 PC에 취약점을 악용하여 몰래 악성코드를 설치한다. 이러한 Exploit kit 계열의 악성코드가 2014년에는 급증한 것으로 나타났다.

셋째, 소셜네트워크를 표적으로 하거나 전파하는 악성코드가 지속적으로 나타나고 있다. 특히 2014년

에는 페이스북이라는 단 하나의 소셜네트워크를 대상으로 한 악성코드가 널리 확산된 것은 상당히 특이한 현상이다. 북미, 중동 페이스북 사용자의 악성코드 감염 현상이 두드러졌다. 이러한 소셜네트워크를 이용한 악성코드 감염은 전파력이 뛰어나다는 점에서 상당한 보안위협으로 자리 잡고 있다[9].



(그림 1) 전 세계 악성코드 유형 분석

3.2 중소기업 대상 악성코드 감염 유형

중소기업기술지킴센터에서는 중소기업 대상으로 악성코드 탐지 및 조치 지원을 위해서 악성코드 탐지 솔루션을 지원하고 있으며 843개 중소기업의 2,495개 PC에 프로그램을 설치하여 악성코드 탐지와 탐지된 악성코드의 조치를 지원하고 있다. 2014년 8월부터 2015년 7월까지 악성코드 탐지 및 조치된 현황은 168,695건이며 이 중에서 위험응용은 99,292건으로 가장 많았고 그 다음으로 이메일, 바이러스, 스파이웨어, 기타 순으로 나타났다. 특히 위험응용과 유사한 이메일을 통한 악성코드 감염까지 합친다면 위험응용을 통한 악성코드 감염은 더욱 큰 폭으로 증가 할 것이다.

위험응용 중 가장 크게 많이 탐지된 유형은 Trojan.Generic. 계열이 가장 많았고 감염경로는 정확하지 않으나 가장 의심되는 부분은 이메일과 보안에 취약한 인터넷 사이트를 통해 감염된 것으로 추정된다. Trojan.Generic. 계열의 악성코드는 자체 전파 기능은 없으나, 악성코드 제작자에게 사용자의 개인정보를 전송하거나 사용자가 입력하는 키보드 입력값을 가로채어 전송할 수 있다. 또한 다양한 악의적인 스크립트를 실행하기 때문에 인터넷 접속이 자주 끊기며, 일부 프로그램이 실행 중 오류가 발생할 수 있고 안티바이러스 같은 프로그램을 못 사용하게 할 수도 있다.

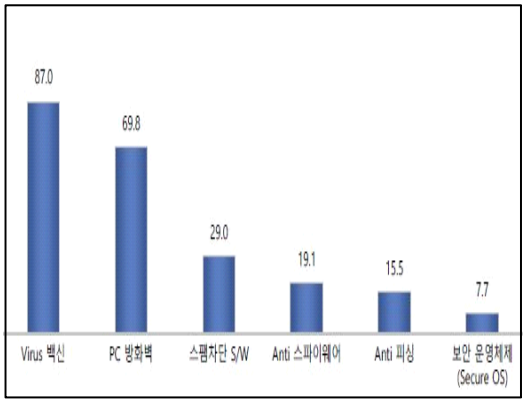
<표 2> 악성코드 종류별 특징 분석

구분	2014년 8월 ~ 15년 7월				
	위험응용	스파이웨어	이메일	기타	합계
개수	99,292	26,431	29,396	13,576	168,695
백분율	59	16	17	8	100

스파이웨어 부문은 검색도우미 관련 스파이웨어가 가장 많이 설치되었으며, 이러한 스파이웨어가 설치되면 툴바에 특정한 아이콘이 생성되고 인터넷 시작 페이지 변경이 가능하다. 또한 팝업광고를 출력하거나 주소표시줄을 감시하고 원하지 않는 주소로 변경하는 등의 여러 가지 악의적인 목적으로 사용할 수 있다. 기타 부문은 보안업데이트 실패, 시스템 이상 시 실패 로그 생성 등 시스템 상의 특이사항을 나타낸다.

3.3 안티바이러스를 이용한 중소기업의 악성코드 대응 문제점

한국인터넷진흥원에서는 해마다 우리나라 정보보호실태를 조사하는데 2014년 정보보호실태조사에 따르면 기업들은 시스템 보안 제품군 중에서는 바이러스 안티바이러스를 사용하는 비율이 87%로 가장 높았으며, 다음으로 'PC 방화벽' 제품이 69.8%, 스팸차단 소프트웨어가 29.0%로 조사되었다[10].



(그림 2) 시스템 보안 제품 사용률

그러나 중소기업기술정보진흥원의 중소기업 기술보호 역량 및 수준조사에 따르면 OS,안티바이러스 등 최신버전업데이트는 대기업이 95.3%이고 중소기업은 71%로 대기업과 20%이상 차이가 나고 있다. 또한 악성코드 감염 등 사고 발생 시 대응절차는 대기업은 구체적으로 마련되어 있다는 답변이 62.8%, 중소기업은 23.5%으로 나타났다. 또한 정기적으로 검사 및 감사가 이루어지는 경우는 대기업이 67.4%이고, 중소기업이 19.3%로 거의 3배 이상의 차이가 발생하고 있다[11].

<표 3> 악성코드 종류별 특징 분석

구분	대기업	중소기업
최신업데이트	95.3	71
사고대응절차 구체적 마련	62.8	23.5
정기적인 검사	67.4	19.3

위 통계자료를 바탕으로 보면 중소기업은 안티바이러스만 설치하고 관리를 전혀 안하고 있는 것으로 나타났다. 이러한 중소기업의 지속적인 보안 관리를 위해서 중소기업기술지킴센터에서는 악성코드탐지서비스를 중소기업 대상으로 무상으로 지원하고 있다.

4. 중소기업의 악성코드 대응 방안

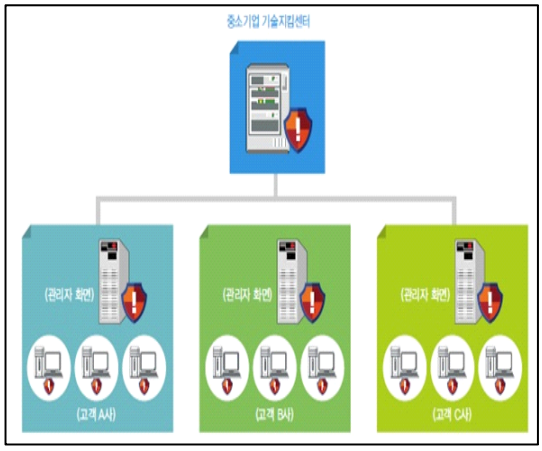
중소기업의 경우 인터넷 사용 시 불명확한 사이트 방문을 제한하거나, 유입되는 악성코드를 막을 수 있는 보안솔루션이 없기 때문에 악성코드에 무방비로 노출되어 있는 측면이 강하다. 또한 보안전문가 부재로 인해 악성코드에 대해 대응도 어려운 실정이다. 중소기업 환경에 적합한 중소기업기술지킴센터의 악성코드탐지서비스를 통해 중소기업의 악성코드의 탐지 및 조치의 어려움을 해결 할 수 있다.

4.1 중소기업기술지킴센터의 악성코드 탐지 방안

중소기업은 보안담당자 부재로 인해 악성코드 감염 시 조치 및 대응에 어려움이 있다. 이러한 문제점을 해결하기 위하여 중앙서버에 관리 프로그램을 배치하고 악성코드 탐지프로그램을 중소기업에 배포하여 중앙서버의 관리프로그램을 통해 24시간 모니터링 및 악성코드 감염 시 조치를 지원하는 방식의 보안관제형 악성코드 탐지가 중소기업에는 적합하다.

이러한 중앙집중형 방식의 보안관제형 악성코드탐지는 중앙에서 중소기업의 PC를 모니터링하고 보안정책 생성 및 배포, 정책관리, 악성코드 감염 내역, 보안위협 현황 및 중앙관리 등을 통해 중소기업의 PC에 대해 직접적인 통제가 가능하다. 중소기업의 관리자들은 PC 보안 현황에 대해 보고서 형태로 제공받아 해당기업의 PC별 보안상황에 대해 손쉽게 파악 할 수 있다.

보안관제형 악성코드 탐지는 악성코드탐지 프로그램의 방화벽 기능 및 침입차단 기능을 통해 1차적으로 네트워크 위협으로부터 시스템을 보호 할 수 있고 최근 급증하는 이메일 악성코드 위협에 대해 이메일 필터링을 통해서 대응할 수 있다. 또한 중요시스템의 보안업데이트 현황 파악을 통해 업데이트를 실시간으로 시행하여 중소기업 시스템의 보안수준을 향상 시키는데 크게 이바지 할 수 있다.



(그림 3) 보안관제형 악성코드 탐지 설계

4.2 중소기업기술지킴센터 악성코드 탐지의 향후 발전 방향

중소기업기술지킴센터의 악성코드 탐지는 중앙집중형 방식의 보안관제형으로 중앙에서 모든 것을 관리해 주고 지원할 수 있다는 장점이 있으나, 단순 안티바이러스 기능에만 의존하고 있어 새로운 악성코드 출현 시에 탐지 및 대응의 어려움도 존재한다. 이러한 단점을 보완하기 위해 다양한 방식의 악성코드 탐지 방법을 접목하고 빅데이터 시스템을 활용한 융합형 악성코드 탐지기술을 추구 해 나가야 할 것이다.

첫째, 행동기반의 악성코드 탐지 시스템을 구축해야 한다. 이 시스템은 기존의 시그니처 기법이나 heuristic 기법이 아니다. 프로세스를 모니터링 하여 해당 프로그램의 악성코드 여부를 결정 후 해당 프로그램을 차단하는 방식으로 기존에 알려진 악성코드와 새로운 악성코드도 탐지가 가능하다[12].

둘째, 가상화를 통한 신종 악성코드 시뮬레이션 예측 기법을 개발해야 한다. 기존의 패턴기반, 시그니처 방식의 정적인 탐지에서 알려지지 않은 새로운 방식의 위협을 탐지할 수 있는 가상화를 이용한 탐지 방식으로 전환해 나갈 필요가 있다. 악성코드 감염은 웹, 메일 등의 다양한 경로를 통해 감염이 진행되고, 공격자들은 공격을 수행하기 위해 다단계의 절차에 따라 공격을 수행한다. 이처럼 다단계로 공격을 하게 되면, 시그니처 방식과 블랙리스트 방식을 사용하는 보안 솔루션은 무력화 되어 해당 공격을 탐지할 수 없다 .이러한 신종 악성코드를 진단하고 대응하기 위해서는 가상화 방식의 시뮬레이션 예측이 필요하다. 가상화 시뮬레이션 예측을 통해 공격자의 목적과 공격 방식을 파악하여, 해당 위협을 실시간으로 탐지하여 조치 할 수 있다[13].

셋째, 빅데이터 시스템을 통해 다양한 로그를 분석하여 새로운 악성코드를 탐지할 수 있다. 빅데이터 시스템으로 로그 수집 및 분석을 통해 정상행위를 미리 정하고 해당 범위를 넘어가는 비정상행위를 탐지할 수 있다. 정상행위를 정하는 기법에는 통계적인 수치 분석을 통해 비정상적인 행위를 탐지하는 통계적(Statistical)방법, 일정 기간 동안 사용자의 모든 로그를 기록하고, 그 기록을 사용하여 규칙을 만들어 현재의 행위를 비교하는 방식인 전문가 시스템(Expert System), 자동학습이 가능한 신경망(NeuraNetworks), 서비스의 정상적인 행위를 기록하고 모든 system call의 정상 시퀀스가 포함된 참조 테이블을 해당 시퀀스를 비교하는 방식인 컴퓨터 면역 시스템(Computer Immune System), 확률값을 이용한 HMM(Hidden Markov Models), 대량의 데이터로부터 필요한 정보를 추출하는 데이터 마이닝(Data Mining) 등의 방식을 이용하여 빅데이터 분석 시스템을 구성하여 새로운 악성코드에 대응 할 수 있다[14].

5. 결 론

본 연구는 중소기업기술지킴센터에서 실시하고 중앙형 보안관제 악성코드 탐지를 통해 1년 동안 탐지된 악성코드 유형 분석을 하였고 해당 악성코드 탐지 방식의 우수성과 향후 발전방향을 제시하였다. 중소기업은 대기업 및 공공기관에 비해 보안투자 부족, 보안전문가 부재 등 여러모로 다른 환경이다. 이러한 중소기업에 단지 보안투자 지원금을 투입한다고 해서 큰 효과를 기대하기 어렵고 관리의 불편함도 따른다. 이러한 중소기업에게는 중앙차원의 메인컨트롤 타워에서 24시간 탐지 및 조치·관리를 지속해 주는 방식이 더 적합하다.

중소기업기술지킴센터에서는 중소기업들을 위해서

중앙 보안관제 악성코드탐지서비스를 제공하고 있으며 관리자가 부재한 중소기업의 PC 및 시스템에 대해 24시간 모니터링을 통해 악성코드 감염 시 통보 및 조치를 지원하고 있다. 중소기업기술지킴센터를 통해 2014년 8월부터 2015년 7월까지 약 17만 건의 악성코드 감염이 탐지되었으며, 이러한 수치는 하루에 465건 정도의 악성코드 감염을 발견하여 중소기업에 통보하고 조치를 지원하고 있는 것이다. 이러한 악성코드탐지서비스를 제공받지 않았다면, 중소기업은 악성코드 감염 사실을 확인 할 수도 없고, 안티바이러스를 통해 감염 사실을 발견해도 보안 전문가 부재로 인해 완전한 조치를 취하기가 어려운 실정이다. 악성코드 감염에 따른 조치에 있어서는 중소기업은 사각지대이다.

중소기업기술지킴센터의 악성코드 탐지서비스는 24시간 모니터링을 통해 공휴일 및 야간에도 악성감염 시 즉각적인 통보 및 조치를 하고 있다.

이러한 중소기업기술지킴센터가 더욱 발전하기 위해서는 중소기업 환경에 적합한 다양한 악성코드 분석 기술, 행동기반의 악성코드 탐지 시스템 구축, 가상화를 통한 신종 악성코드 simulation 예측 기법 개발, 빅데이터 분석 시스템 개발 등 다양한 방식을 지속적으로 연구·개발 해 나갈 필요가 있다.

참고문헌

[1] ITU, "itu statistics 2014", 2014.

[2] 한국인터넷진흥원, “2014 한국 인터넷 백서”, pp.369, 2014.

[3] 김창희, “전자금융거래의 보안 위협과 대응 기술”, 개인정보보호컨퍼런스, 2010.

[4] 홍준석, 임영환, 박원형, 국광호, "중소기업 유해 트래픽 분석을 통한 보안관제 개선 방안", 한국전자거래학회지, 제19권, 제4호, pp. 195-204, 2014.

[5] Malware, http://en.wikipedia.org/wiki/Malware, 2014

[6] 안성진, 이경호, 박원형, 보안관제학, 이안미디어, 2014

[7] 임원규, 이정현, 임수진, 박원형, 국광호", 윈도우 악성코드 분석을 통한 탐지 및 대응 기술에 관한 연구", 융합보안논문지, 제10권, 제1호, pp. 19-27, 2010.

[8] 임원규, 이정현, 임수진, 박원형, 국광호, "APT 공격과 대응 방안 연구", 융합보안논문지, 제5권, 제1호, pp. 25-30, 2015.

[9] F-Secure, “2014 THREAT REPORT”, 2014.

[10] 한국인터넷진흥원, 2014년 정보보호실태조사(기업부문), 2014

[11] 중소기업기술정보진흥원, 2013 중소기업 기술 보호 역량 및 수준조사, 2013

[12] 김성우, 신재인, 방영환 , "행위 기반 악성코드 탐지 차단 시스템 개발", 보안공학연구논문지, 제9권, 제2호, pp. 163-176, 2012.

[13] FireEye , “지능형 표적 공격 차세대 사이버 공격을 방어하는 방법”, 2013.

[14] 임설화, 김종수, 양준근, 임채호, "APT 현황과 신종 악성코드 대응방안", 정보보호학회지, 제24권, 제2호, pp. 63-72, 2014.

[저 자 소 개]

홍 준 석 (Jun-seok Hong)

2002년 2월 경영학사
2012년 8월 공학석사
2013년~현재 서울과학기술대학교
IT정책전문대학원
산업정보시스템공학 박사과정

email : hjsjun0817@naver.com

김 영 희 (Young hee Kim)

2001년 컴퓨터공학사
2001년~현재 인터파크, 한화S&C
2013년 산업정보시스템공학석사
2014년~현재 서울과학기술대학교
IT정책전문대학원
산업정보시스템공학 박사과정

email : sorak75@naver.com

박 원 형 (Wonhyung Park)

2002년 서울과학기술대학교
산업정보시스템공학과
공학사
2005년 서울과학기술대학교
정보산업공학과
공학석사
2009년 경기대학교 정보보호학과
이학박사
2015년 성균관대학교 교과교육학
교육학박사 수료
2012년~현재 극동대학교 사이버안보
학과 교수/학과장

email : whpark@kdu.ac.kr

국 광 호 (Kwang-ho Kook)

1979년 서울대학교 산업공학사
1981년 서울대학교 대학원
산업공학석사
1989년 미 조지아 공과대학교 대학원
산업공학박사

email : hkook@seoultech.ac.kr