중소기업융합학회 논문지 제5권 제1호 pp. 13-18, 2015 ISSN 2234-4438

악성코드의 위협과 대응책

임동열
백석대학교 정보보호학과*

Threats and countermeasures of malware

Lim Dong Yul*
School of information security and Baek seok University

요 약 악성코드란 해커가 악의적인 목적을 위하여 작성이 되어있는 실행 가능한 코드의 통칭으로써 자기복제 능력과 감염 대상 유무에 따라 바이러스, 웜, 트로이목마 등으로 분류된다. 주로 웹페이지 검색이나 P2P사용, 셰어웨어를 사용 할 때 등, 이런 상황에서 침투가 많이 발생이 되고 있다. 악성코드로 공격을 당하게 되면 이메일이 자동으로 발송이 된다거나, 시스템 성능 저하, 개인 정보 유출 등의 피해를 입게 된다. 이번에 악성코드를 소개 하면서 악성코드에 관련된 내용들을 설명하고 대응책을 알아본다. 그리고 향후 연구방향에 대해서도 생각해본다.

주제어 : 악성코드, 바이러스, 웜, 트로이목마

Abstract The malware, as hackers generic name of executable code that is created for malicious purposes, depending on the presence or absence of a self-replicating ability infected subjects, and are classified as viruses, worms, such as the Trojan horse . Mainly Web page search and P2P use, such as when you use a shareware, has become penetration is more likely to occur in such a situation. If you receive a malware attack, whether the e-mail is sent it is automatically, or will suffer damage such as reduced system performance, personal information leaks. While introducing the current malware, let us examine the measures and describes the contents related to the malicious code.

Key Words : malware, virus, worm, trojans, Penetration

1. 서론

악성코드(Malware)란? 해커가 악의적인 목적을 위하여 작성이 되어있는 실행 가능한 코드의 통칭으로써 자신을 복제하는 능력과 감염이 될 대상이 있는지 상황에 따라 웜(Worm), 바이러스(Virus), 트로이목마(trojans)등으로 분류된다. 주로 웹페이지검색이나 P2P사용, 셰어웨어를 사용할 때 등, 여러 상황에서 침투가 많이 발생이 되고 있다.

악성코드를 이용하여 공격하는 대표적인방법 으로는 메일을 자동으로 발송 하는 방법과, 시스템의 성능을 저하시키는 방법, 개인정보를 유출하는 방법 등이 있다. 나날이 갈수록 해커들이 늘어나면서 위에 소개된 방법 외 여러 가지 방법을 가지고 악성코드를 피해를 입히고 있다. 본 논문에서는 이러한 악성코드공격에 대해서 상세하게 알아보고, 허니팟(Honeypot)기술을 통하여 시스템을 구축하여 악성코드의 침입을 탐지해 본다, 예방하는 방법에 대해 알아본다.

Received 2015-02-21 Revised 2015-03-07 Accepted 2015-03-14
*Corresponding author : Lim Dong Yul (Limdongyul@naver.com)

2. 악성코드(Malware)의 종류

본 장에서는 해커들이 많아지면서 늘어나고 있는 악성코드 Fig. 1. 을 정리하고, 특징과 종류를 파악하고 분석한다. 악성코드는 악의적인 목적을 가지고 시스템의 성능을 저하시키거나, 정보를 빼내는 등의 행위를 하기 위하여 사용자 몰래 컴퓨터에 접근하는 행위와 프로그램이 설치가 되는 행위들로 정리를 할 수가 있고, 늘어나고 있는 해커와 발전하는 악성코드를 분석을 통하여 특징을 파악하고 이에 따른 탐지 및 분석 기법을 알아본다.

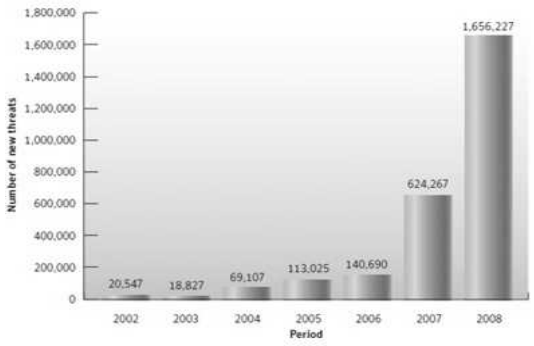

Fig. 1. Internet Malware

2.1 악성코드 분류

악성코드는 활동하는 목적에 따라서 이를 차단 및 탐지방법이 여러 가지로 나뉘게 된다. 본 절에서는 악성코드에서 이루어지는 행위를 보고 분류를 하여 이에 따른 종류를 나누어 본다.

2.1.1 Virus

Virus는 컴퓨터 시스템에 몰래 침투를 하여 바이러스가 실행이 가능한 파일이나 기생하고 있는 프로그램에 자신이나 변질된 자기 자신을 감염시킨 다음에 다른 상대를 찾아 감염을 시킨다. 이 코드 혹은 프로그램이 시스템이나 파일을 파괴한다. Virus는 컴퓨터를 비정상적으로 동작을 하게하고, 데이터를 지우거나, 인터넷 속도를 느리게 하거나, 컴퓨터 성능을 안 좋게 하는 등의 나쁜 행위들을 한다.

2.1.2 Worm

Worm은 자신을 복제한다, 그리고 파일이나 숙주프로그램이 없이 자신이 혼자 실행된 후 프로그램 내에서 컴퓨터와 컴퓨터 사이 또는 프로그램과 프로그램 사이를 이동면서 확산시키고, 자기 자신을 스스로 복제하며, 컴퓨터 내부 기억장소에 실행파일이나 코드의 형태로 존재하는 프로그램 조각이다. Worm바이러스는 자신을 스스로 복제, 사용자가 인식하지 못 하도록 몰래 이메일 전송, 해당 개발사나 프로그램 내에서 제공하지 않는 멀쩡한 파일에 새로운 코드 삽입 등 악의적인 행위들을 한다. Virus가 자기복제가 가능한 것처럼 Worm도 자기 복제가 가능하다. 하지만 이 둘의 사용되어지는 방법에 대한 차이점이 있다. Worm은 자기 자신 그 자체로도 네트워크를 통하여 전파를 할 수가 있고, Virus는 파일에 삽입이 되어 사용된다.

2.1.3 bot

Bot은 공격대상의 컴퓨터를 해커가 제어하도록 만들어 주는 프로그램이다. Bot Master의 명령에 따라 여러 경로로 공격대상의 컴퓨터에 침입하여 명령에 따른다. 감염이 된 컴퓨터를 자유자제로 제어를 할 수 있고 컴퓨터에 저장된 정보를 수집할 수 있기 때문에 정보 유출을 할 수 있고, 다른 시스템을 공격하는 데 사용되는 것이 Bot Master이다. 이러한 Bot들이 네트워크를 형성한 경우를 botnet이라 부른다.

2.1.4 Trojan Horse

Trojan Horse는 악성루틴을 포함하고 있고 하나의 정상적인 프로그램형태로 위장을 하고 있는 프로그램이며 사용자가 다른 프로그램 내에서 알 수 없도록 포함되고, 자기 자신을 복제하지는 못한다. Trojan Horse는 자기 자신을 복제할 수 없고 해커가 일부러 삽입을 시킨다. 이 때문에 버그와도 다르기 때문에 Virus나 Worm과는 다른 특성을 가지고 있다. 주요 행위로는 DDos공격이나 Key Logging을 이용한 사용자의 ID 나 Password를 수집하거나 Back door설치 등, 최근에는 GameHack으로 사용하는 경우도 있다[9]. Fig. 2.에 의하면 Trojan Horse는 다른 파일을 감염 시키지 못하고, 공격대상이 직접 실행하도록 하여 자기 스스로 피해를 입도록 한다. Virus가 정상적 파일이나 정상적 Boot영역 등을 감염시키며 전파가 된다는 점에서 차이가 있다.

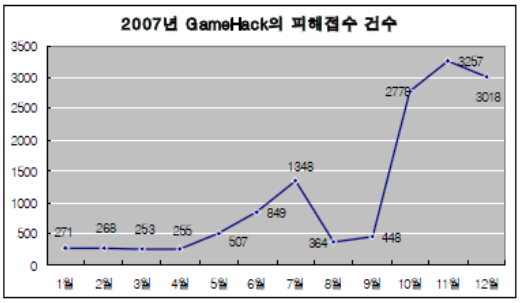

Fig. 2. Trojan Horse Victims Analysis

2.1.5 Root-kit

Root-kit이란 시스템에 전반적으로 접근할 수 있는 루트(Root) 권한을 쉽게 얻게 해주는 킷(Kit) 이라고 쉽게 해석이 가능하다. Root-kit은 소프트웨어나 펌웨어에 침투한 후 자신을 침투된 시스템의 관리자인 것처럼 하는 악성행위, 파일의 내용을 바꾸거나 원래의 운영체제를 가상화시키는 악성행위 등을 수행한다.

2.1.6 Backdoor

Backdoor는 정상적인 인증을 통하여 시스템 내에 접근하는 것이 아니고 시스템의 자원이나 시스템의 자료를 빼내기 위하여 해킹을 한 후 다음에 접속을 할 때 쉽게 접속을 하기 위한 시스템의 보안이 제거된 비밀 통로이다. 즉, 최초 공격자가 시스템에 침입을 한 후, 해커가 침입하고 싶을 때 침입을 할 수 있고, 권한이나 정보를 쉽게 빼내기 위한 비밀 통로라고 볼 수 있다.

2.1.7 Key-logger

Key-logger는 공격대상의 키보드로부터의 움직임을 탐지하고 감시를 통해 기록하여 해커에게 전송해주는 공격이다. Key-logger가 감염된 컴퓨터의 공격대상이 키보드를 이용하여 입력하는 ID나 Password, 계좌번호, 주민등록번호, 카드번호 등과 같은 중요한 정보를 몰래 빼내가는 해킹공격이다.

2.1.8 Spy-ware(Spy Software)

Spy-ware는 인터넷에서 무료로 다운받을 수 있는 프로그램에 주로 포함이 되어있다. 사용자의 동의를 받지 않고 감염된 네트워크나 컴퓨터를 통해서 기업이나 개인에 대한 정보를 수집을 함으로써 공격대상에게 전송하도록 만들어진 프로그램이다. 계정 정보나 금융정보, 개인정보와 같은 여럿정보나 데이터 등을 수집하는 해킹이다.

2.1.9 Ad-ware(Advertising-supported Software)

Ad-ware란 사용자의 컴퓨터의 초기화면을 특정사이트로 고정을 시키거나 광고성 팝업창을 띄우는 사용자가 의도하지 않는 행위 및 정보를 실행 가능한 코드를 수행하게 하는 프로그램이다. Ad-ware의 가장 큰 문제점은 사용자가 불편함을 느낀다는 것 이다. 팝업창 띄우기, 인터넷의 시작페이지를 변경하거나, 고정을 하는 등의 불편함을 유발한다[1].

3. 악성코드 분석 및 기술동향

악성코드의 수가 기하급수적으로 증가하고 있다. 급속도로 증가하고 있는 악성코드들을 하나하나 일일이 수집하거나 분석하는 것은 현실적으로 힘들고 불가능한 일이다. 왜냐하면 해커가 많아지면서 악성코드의 수가 증가하는 반면에 분석을 할 수 있는 인력은 적기 때문이다. 그러므로 수동으로 악성코드를 분석하기보다는 어떻게든 다동으로 악성코드를 분석하는 방법을 강구하게 되었다. 또 다른 분석의 어려움은 대부분의 악성코드들이 적용하고 있는 분석방해 기법에 있다. 분석방해 기법을 무력화 또는 우회를 하여야 분석을 할 수 있다. 이를 예방하기위해 동적분석기법에 대한 많은 연구가 진행이 되고 있다, 동적분석기법에 대표적인 기술로는 ThreatExpert, Botwall , CWsandbox, Norman Sandbox가 있다. 이런 분석시스템들의 분석 방식을 보면 악성코드를 일부러 수행하여 수행된 악성코드의 파일, 프로세스, 레지스터, 네트워크 등과 관련된 행위 정보들을 모니터링한다. Table 3 동적분석 제품들의 특성에 대한 비교내용이다. 또한 제품특성 및 대표적 동적분석기술을 분석한 것이다.

Table 3. Dynamic Analysis Comparison

분석도구 / 주요 특징	ThreatExpert	Botwall	Norman Sandbox	CWsandbox
분석 플랫폼	가상머신	에뮬레이터	자체플랫폼	가상머신
판매 형태	무료	상용	상용	무료/상용
분석 가능 파일 포맷	EXE	EXE	EXE	EXE, 오피스파일

악성코드는 이제 실행파일 형태로만 배포되는 것이 아니라 PDF파일, Word파일, PPT파일 Excel파일등 다양한 형태로 만들어져 배포되고 있다. 이와 비슷한 현상으로 Adobe의 취약점이 공개가 되고나서 Adobe를 대상으로 하는 악성코드들이 많이 나타는 것을 보면 확인할 수 있다. 최근 악성코드 분석 기술을 보면 PDF파일이나 PE파일 등과 같은 다양한 타입의 악성코드를 분석 Fig. 3. 할 수 있는 기능을 일부 제공되거나 개발되어지고 있다. [2]

Fig. 3. PDF Vulnerability Analysis

3.1 악성코드 동향

최근 몇 년간 악성코드는 과거의 몇 년에 비해 질적으로나 양적으로 비약적인 성장했다고 느낄 수 있다. 양적인 성장은 그림[Fig. 3-2]를 보면 알 수 있으며 이와 함께 악성코드의 영역이 직접적인 실행파일이 아닌 PDF등과 같은 문서 파일을 포함한 보다 넓어 졌다는 것을 통해 인식을 할 수가 있다. 최근 악성코드들은 감염 호스트에 오래 있는 것이 이익이므로 Rootkit 기법을 적용한 악성코드들이 등장하고 있으며 발견되더라도 분석이 용이하지 않도록 Anti-debugger. Anti-VM 등과 같이 분석 환경을 탐지 하는 기능들을 포함한 악성코드들도 있다. 또한 최근엔 다양한 기능을 가지고 있는 Software들이 많이 있다. 이로 인해 악성코드는 이제 전문가가 아닌 일반인들도 만들어낼 수 있다. 그러므로 악성코드는 누구나 만들 수 있는 Software를 통하여 만들 수 있으므로 전반적인 수준도 함께 성장하였고 악성코드의 수준 향상은 분석을 더욱이 힘들게 하고 있다.[8]

4. 허니팟(Honeypot)

허니팟은 컴퓨터에 침입한 바이러스나 스팸과 같은 악성코드를 탐지하는 가상으로 만든 컴퓨터이다. Fig. 4. 에 의하면 실제로 공격을 당하는 것처럼 보여서 정보를 수집하고 침입자를 추적하는 역할을 하는 최신 침입탐지 기법이다. 허니팟의 명칭의 유래는 꿀단지를 침입자를 유인하는 함정으로 비유함에서 나왔다.[3]

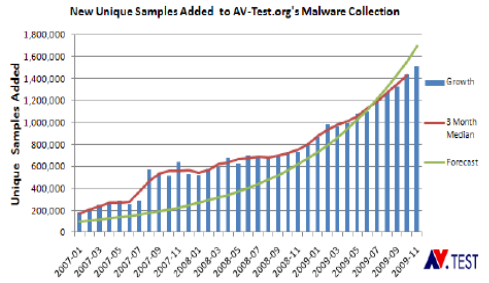

Fig. 4. Malware Increasing Trend

4.1 허니팟 관련연구

기존 허니팟 연구는 크게 두 가지로 구분할 수 있다. 하나는 허니팟 시스템을 이용하여 공격을 유인하되 내부 시스템이 공격받지 않도록 하는 시스템이며, 다른 하나는 유도한 공격의 로그를 수집하여 향후 공격시에 대응하는 방법기법을 연구하는 목적을 가진 허니팟으로 구분된다.[4]

4.1.1 공격목적의 허니팟

허니팟 개발 초기의 목적에 맞는 허니팟으로써, 크래커의 침입을 스스로 일으키도록 유도하여 보호해야 할 자산이 있는 내부시스템을 보호하는 목적을 가지고 있다. 허니팟은 쉽게 해커에게 노출이 되어야한다. 또 마치 취약한척 해킹이 가능한 것처럼 보여야한다. 또한, 관리자는 이 허니팟에 접속하는 이용자들을 확인할 수 있도록 구성되어야 하고 시스템을 통과하는 모든 패킷들을 감시할 수 있어야 된다. [4]

4.1.2 방어목적의 허니팟

방어목적의 허니팟은 일부러 공격을 받기위한 기본 기능을 가지고 있고, 더 앞서나가 해커들의 방법들과 행동에 대한 정보들을 수집하는 것을 목적으로 하고 있다. 실제로 크래커들을 유인하여 실제 서비스 네트워크와 격리된 상태로 실제와 같은 네트워크를 제공해서 실제 서비스 네트워크 인 듯 속인다. 허니팟 한 대로는 크래커의

유도가 쉽지 않다. 따라서, 여러개의 허니팟으로 이루어진, 허니넷(Honeynet)을 구성하는 연구가 활발하게 진행되어지고 있다 [4].

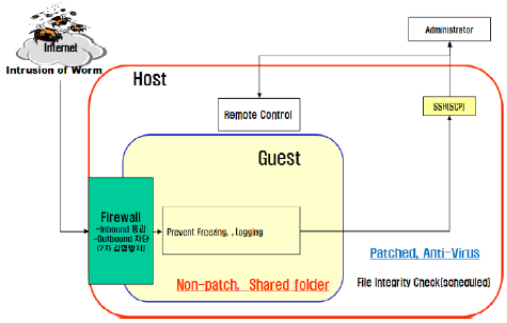

Fig. 5. Configuration of Honeynet

4.2 허니팟 시스템 구축

4.2.1 호스트 시스템 구성

허니팟 시스템을 구성하는데 있어 공격대상을 가상서버로 운영을 한다. 가상서버를 사용하는 주목적은 악성코드에 감염이 된 후에도 시스템 복구가 쉽다는 장점 때문이다. 구축된 가상 호스트 시스템은 시스템 보호를 위해 최신 보안 패치를 설치하고, 자동 업데이트 기능이 활성화된 O/S를 사용한다. 또한 바이러스를 감지할 수 있는 시스템을 설치를 하여 보안 수준을 높인다. 또 관리를 효과적으로 하기 위하여 Active Perl을 설치하여 [table. 4-1]과 같은 Script를 실행 할 수 있도록 설정을 한다. 본 장에 기술한 환경은 기존에 다른 연구에서 사용되었던 방법이다.

4.2.2 피 공격용 시스템 구성

호스트 시스템의 Guest 시스템으로 동작하는 피 공격용 시스템은 악성코드 유입이 쉽게 될 수 있도록 보안패치가 되지 않게 하고 침입한 악성코드가 외부 네트워크로 유포되는 것을 막을 수 있도록 설치한다. 본 장에서 구성한 전체적인 허니팟 시스템의 구조는 그림 [Fig. 4-3]처럼 나타난다. 피 공격 시스템이 악성코드에 감염이 되면 CPU 사용률이 100% 상태를 유지할 수 있고, 이를 해결하기 위하여 프로세스를 강제적으로 종료시킬 수 있는 유틸리티를 설치를 한다. 또한 수집된 악성코드를 호스트 시스템으로 보내기 위해 공유 폴더를 설정한다. 스케쥴 프로그램을 이용하여 특정 주기로 악성코드가 호스트 시스템에 자동으로 기록이 된다[5].

Table 4. Type of Scripts running on PC

파일명	설명
Startvm.bat	Guest PC 시작
Stopvm.bat	Guest PC 중지
Validate.bat	악성코드 샘플의 PE Validation 체크
archive	악성코드 샘플 압축

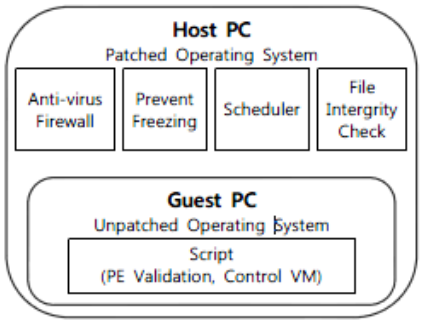

Fig. 6. Honeynet System Configuration

5. 대응방안

분석 내용을 토대로 대응방안을 살펴보고자 한다. 악성코드로부터의 보안을 위해서는 “예방-탐지-대응”이라는 과정을 거치는 것이 좋다. Fig. 6. 를 통해 세 과정의 주요 내용을 알 수 있다. “예방”은 평소에 정보보호를 위해 하는 활동을 의미한다. 예를들어 방화벽이 있다 [6]. 다음으로 ‘탐지’는 공격에 대한 징후를 탐지하는 단계이다. 마지막으로 ‘대응’은 악성코드에 감염이 된 후 얼마나 신속하게 대처하고 피해를 최소화고 2차적 피해를 감소시키는 활동이다 [7].

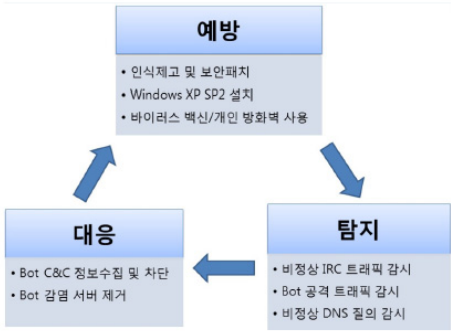

Fig. 6. Anti-Malware Configuration

* 1) 대응방안

5.1 효과적인 대응방안

최근 악성코드 공격은 국경과 상관없이 넓은 반경으로 분포가 되어있다. 다양한 악성코드에 의해 공격은 수행이 된다. 즉 특정한 망을 통하여 사용자는 공격에 의하여 피해를 받을 수 있다. 악성코드 공격에 대한 예방 측면에서 악성코드의 정확한 규모를 파악해야 하고, 악성코드의 분포 및 구성을 흐트려 놓기 위해서 여러 가지의 도메인에서의 악성코드 관련 탐지정보가 통합되어야 전체 구성 및 규모를 파악할 수가 있다. 악성코드를 통한 공격이 발생했을 때 효과적인 대응책을 위해 도메인간 서로 도움을 줘야한다. 개인정보를 공개하지 않으려하는 성향과 서로 복잡한 관계로 인한 서로간의 도움이 어렵고 풀어나갈 문제도 많다. 최근에는 악성코드 국제적인 추세나, 공격양상을 보면, 악성코드공격에 대한 국내·외 서로간의 도움은 지속적인 대화가 이루어지고 있다. 빠른 시일 내에 어떠한 모습으로든 구현을 할 것이라고 예상한다.[2]

6. 결론

앞으로는 더욱더 많은 해커들이 나타날 것이다. 해커들이 증가함으로 인한 악성코드의 증가는 어마어마해 질 것이다. 이에 방어하기 위해서는 먼저 악성코드에 대한 속성을 파악을 해야 한다. 위에 언급되었던 허니팟과 같은 시스템을 활용하여 함정을 만들어 악성코드를 유인을 한다던가, 악성코드에 대하여 더욱더 심도 있게 파고들어야 한다. 5장에 언급되었던 “예방-대응-탐지”라는 과정을 이용하여 피해를 최소화를 시키도록 노력해야 한다. 사실상 일반 사용자 입장에서는 공격에 대한 탐지는 사실상 어렵다고 본다. 앞으로 정보보호학을 전공한 사람들과, 현재 V3, 고클린과 같은 백신을 개발하는 개발자들이 악성코드들을 더욱더 심도 있게 분석하여야 한다. 그래야 일반 PC사용자들은 유료화가 되어도 자신의 컴퓨터 보호를 위해서 사용하게 될 것이다. 그 정도로 보안은 중요한 측면이다. 프로그램 개발자들이 지금도 보안에 힘을 써주고 있고, 새로운 프로그램개발로 인하여 보안은 점점 더 강화가 되어있다. 하지만 악의적인 목적을 가진 해커들 또한 이에 대응하는 악성코드를 만들고 있기 때문에, 악성코드를 더욱더 효과적이고 실용적으로 분석하고 막아주는 프로그램 디자인이 필요할 것이라고 생각된다.

REFERENCES

[1] Kang bu joong other two, malicious code detection technology status and, Hanyang University, 2012

[2] Lim chae tae other two, the latest technology trends and analysis of malicious code Study, National Internet Development Agency of Korea, 2010

[3]http://terms.naver.com/entry.nhn?docId=1233741&cid=40942&categoryId=32848

[4] Heo jong oh, Jo si haeng, Studies on building a global system for malware collection honeypot, AhnLap, 2010

[5] Yi ju hwa other four, research on the collection and use of malicious code method using a honeypot, Samsung Electronics, 2012

[6] Kim so eui other two, detection and response through the analysis of the malicious code, malicious Bot, Korea Communications Society, 2013

[7] http://www.hanb.co.kr/network/view.html?bi_id=645

[8] Sin dong hwi other three, measures for automated static analysis of malicious code research, Sungkyunkwan University, 2010

[9] Jang young joon other three, malware trends and the future outlook, Information Security and Cryptology, 2008

임 동 열(Dong-Yul Lim) [학생회원]

- 2009년 2월 : 용인성지고등학교 졸업
- 2009년 3월 : 백석대학교 정보통신학부 입학
- 2009년 3월 ~ 현재 : 백석대학교 4학년 1학기 재학중
- 관심분야 : 컴퓨터 보안
- E-Mail : limdongyul@naver.com