악성코드 수집을 위한 글로벌 허니팟 시스템 구축에 관한 연구

허종오 ○ 조시행

안철수연구소

maha96@ahnlab.com , shcho@ahnlab.com

A Study on Installation of Global Honeypot System for Collecting Malicious Code

Jong Oh, Hur○ Si Haeng, Cho

AhnLab

요 약

크래커(Cracker)의 공격으로부터 내부 자원을 보호하기 위한 허니팟 시스템은 크게 두 가지로 구분된다. 하나는 내부 정보자원을 보호하기 위해 크래커의 공격을 유인하는 목적의 허니팟이며, 다른 하나는 방어기법을 연구하기 위해 크래커의 공격을 유도한 후 공격기법을 로그기반으로 수집하는 허니팟이다. 하지만, 최근의 공격은 크래커로 인한 공격보다는 불특정 다수를 공격하기 위해 대량의 악성코드를 통한 공격이 주를 이루고 있다. 따라서, 허니팟의 유형도 변화가 필요하게 되었다. 악성코드에 대한 방어기법을 연구하는 Anti-Virus 연구소에서는 최근의 악성코드 공격으로부터 시스템을 보호하기 위해서는 악성코드를 조기에 수집하는 것이 주요 이슈로 등장하게 되었다. 악성코드 수집을 위한 허니팟은 기존 허니팟과 다른 특징을 가지고 있으며, 이러한 특징을 고려하여 개발되어야 한다. 하지만, 악성코드 수집용 허니팟이 필수적으로 갖추어야 할 조건이 정의된 것이 없으며, 개발을 위한 구현 모델이 존재하지 않아, 실제 구축에는 어려움을 겪고 있다. 따라서, 본 고에서는 기존 허니팟과 비교를 통해 악성코드 수집용 허니팟이 갖추어야 할 7대 요구조건을 개발하고, 이를 토대로 기존에 제시된 적이 없는 악성코드 수집용 허니팟 구현 모델을 제안하였다. 또한, 구현 모델을 통해 실제 악성코드 수집용 허니팟을 개발 및 실제 구축하여, 수집 결과와 함께 구축 시 고려사항을 도출하였다. 앞으로, Anti-Virus 연구소들은 본 구현모델과 구현결과, 고려사항을 통해 악성코드 수집용 허니팟을 개발하여, 확산되는 악성코드를 조기에 수집 및 대응함으로써, 1.25 대란, 7.7 DDoS대란과 같이 악성코드로 인해 발생하는 국가적 정보자산 손실을 미연에 방지하는데 큰 기여를 할 것으로 기대된다.

1. 서 론

실제 침입을 당한 것처럼 크래커(Cracker)를 속이기 위해 고안된 허니팟(Honeypot)은 크래커의 침입 기법을 수집하고, 역추적하기 위해 1990 년대 중반 미국 매사추세츠공과대학 교수 데이비드 클록(David Clock)이 처음 제안한 뒤, 2002 년도에 소프트웨어 제조회사 사익(SAIC : Science Applications International Coportation)이 실제 프로젝트를 시행하여, 개발된 침입탐지 시스템이었다. 이를 통해 침입자의 공격으로부터 내부시스템을 보호하고, 침입자의 공격기법 및 행위기법을 로그기반으로 분석하여, 침입자에 대한 방어기법을 연구하며, 실제적으로 행위기반으로 시그니처 등을 제작할 수 있는 정보를 제공하였다.[1-3] 하지만, 근래에 들어서는 특정 크래커의 공격보다는 악성코드 제작툴(Generator, Maker)을 이용하여 네트워크로 확산되는 소프트웨어적 로봇을 의미하는 봇(Bot)과 같은 악성코드를 통해 불특정 다수의 시스템을 공격하는 방식으로 변경되었다.[2] 또한, 로그 분석 등의 기법을 통해서는 다수의 악성코드를 실시간적으로 분석하지 못해 실시간대응(Real-time Response)을 못하고 있다. 따라서, Anti-Virus 연구소들은 2009 년 7.7 DDoS 대란과 같이 대량의 악성코드 공격에 대한 실시간 대응능력을 확보하기 위해, 악성코드 수집용 허니팟 구현의 필요성을 느끼게 되었다.

하지만, Anti-Virus 연구소들은 기존 허니팟과 다른 특징을 가지고 있는 악성코드 수집용 허니팟에 대한 연구

자료가 부족하여 구현에 어려움을 겪고 있다. 따라서, 본 연구에서는 악성코드 수집을 위한 허니팟과 기존 허니팟의 차이점을 파악하여, 기존에 제시된 적이 없는 악성코드 수집용 허니팟이 가져야 하는 요구조건을 제시하고, 이를 바탕으로 악성코드 수집용 허니팟을 구현할 수 있는 구현 모델을 개발하였다. 또한 이 모델을 통해 실제 허니팟을 구현하였으며, 구현한 허니팟을 국내,외에 설치하여 글로벌 환경에서 수집결과를 도출하여, 결과를 통해 악성코드 수집용 허니팟 설치 시 고려해야 할 사항들을 제시하였다. 이를 통해 Anti-Virus 연구소들이 악성코드 수집용 허니팟을 개발함으로써, 악성코드를 조기에 수집하는 능력을 확보하여, 1.25 대란, 7.7 DDoS 대란과 같은 악성코드로 인한 큰 피해를 미연에 방지하는데 기여하고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 관련된 기존 연구들에 대해 알아보고, 3 장에서는 악성코드 수집을 위한 허니팟이 갖추어야 할 주요 요건을 기존 허니팟과의 비교를 통해 도출하였다. 그리고 4 장에서는 요구조건을 토대로 악성코드 수집을 위한 허니팟을 구현하기 위한 구현 모델을 제시하였다. 5 장에서는 구현모델을 통해 실제 악성코드 수집용 허니팟을 구현하였다. 6 장에서는 구현한 허니팟을 국내,외에 설치하여 결과를 여러 가지 측면에서 도출하였으며, 7 장에서는 구현 결과를 통해 허니팟 설치 시 고려사항을 제시하였다. 끝으로, 8 장에서는 결론을 통해 향후 연구계획에 대해 정리하였다.

2.관련연구

2.1 허니팟 관련연구

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

2.1.1. 공격을 유인하는 목적의 허니팟

허니팟 개발 초기의 목적에 부합하는 허니팟으로써, 크래커의 침입을 능동적으로 유도하여 보호해야할 자산이 있는 내부시스템을 보호하는 목적을 가지고 있다.[4] 따라서, 허니팟의 요건으로서는 쉽게 해커에게 노출되어야하며, 해킹이 가능한 것처럼 취약해 보여야 한다. 또한, 시스템을 통과하는 모든 패킷을 감시할 수 있어야 하며, 관리자는 허니팟 시스템에 접속하는 접속자를 확인할 수 있도록 구성되어야 한다.[5-6] 이러한 시스템은 2000 년대 초기에 나온 많은 허니팟이며, 연구결과로 나온 공개 허니팟 툴로는 Trapserver1, BackOfficer Friendly 등이 있다.

2.1.2. 방어기법을 연구하는 목적의 허니팟

방어기법을 연구하는 허니팟은 공격을 유도하는 기본 기능을 내포하고 있으며, 더 나아가 해커들의 행동과 방법에 대한 정보 수집에 목적을 두고 있다. 실제로 크래커들을 유인한 후 실제 서비스 네트워크인 것 처럼 속이기 위해서는 실제 서비스 네트워크와 격리한 상태에서 실제와 동일한 네트워크 환경을 제공해야 함으로, 허니팟 한 대로는 크래커의 유도가 쉽지 않다 따라서, 다수의 허니팟으로 구성된 네트워크 즉, 허니넷(Honeynet)을 구성하는 연구가 활발히 진행되고 있다.[7]

2.2. 악성코드 관련 연구

이와 같이 기존의 허니팟은 크래커의 침입으로부터 내부자원을 보호하기 위해 크래커를 유인하고, 실제 서비스 환경인 것처럼 속여 크래커의 침입 방법 및 행위를 로그기반으로 수집하고자 하는 것이 주 목적이다. 하지만 최근 크래커의 공격방법은 특정 타겟에 대한 공격보다는 금전적 이득을 위해 불특정 다수를 공격하는 방식을 취하고 있다. 이와 같이 다수를 공격하기 위해서는 크래커 홀로 공격이 불가능함으로 악성코드를 제작하여 대량의 공격 방식을 취하고 있다. 이러한 악성코드들이 웜이며, 웜은 주로 시스템의 취약점을 이용하여 네트워크로 전파되고 있다. 따라서, 실제적으로 시스템의 피해를 방지하기 위해서는 이러한 악성코드를 수집/대응 하는 것이 필요하며, 최우선의 방법으로 취약점을 통해 전파되는 악성코드를 수집하는 것이 실제 Anti-Virus 연구소에서는 필요하다. 따라서 다음 장부터는 실제 악성코드를 수집하는 것에 목적을 두는 허니팟 시스템에 대한 특징 및 구현 모델을 알아보자.[8-11]

2.3. 가상화 기술 연구

허니팟 시스템은 취약한 시스템과 관리를 위한 시스템으로 구분되어야 하며, 이러한 기능을 한 시스템에서 수행하기 위해서는 가상화 기반의 시스템을 구축해야 한다. 따라서, 가상화 시스템을 구축하기 위해서는 가상화 기술이 필요하다. 가상화 기술로써는 전가상화(Full-Virtualization) 반가상화(Para-Virtualization) 기술이 있으며, 두 기술 모두 VMM(Virtual Machine Monitor)기술에 기반을 두고 있다. 차이점으로 전가상화는 이진코드 변환기법(binary code translation)을 사용하는 VMM 위에서 서로 다른 Guest OS(Linux, Windows, Solaris, Netware 등)을 갖는 다수의 가상머신을 실행하는 구조로서, Guest OS 를 수정할 필요가 없다. 유형으로는 VMware 의 ESXi, Microsoft 의 Virtual PC, Window7 의 가상화 기능, KVM 등이 있으며 반가상화는 전가상화의 하드웨어 에뮬레이션으로 인한 성능 저하의 단점을 보완하였으나, 하드웨어 API 를 직접 Guest OS 에 반영하기 위해 Guest OS 를 수정해야 한다. 유형으로는 캠브리지 대학의 연구프로젝트로 시작한 Xen 이 있다. [10-12]

3. 악성코드를 수집하는 허니팟의 요구조건

본 장에서는 기존 허니팟과 악성코드 수집용 허니팟의 특징을 비교하여 악성코드 수집용 허니팟이 필수적으로 갖추어야할 요구조건을 설명한다.

3.1. 기존 허니팟과 악성코드 수집용 허니팟 비교

악성코드 수집용 허니팟은 기존 허니팟과 다른 특징을 가지고 있으며, 최소 사양을 기반으로 기존 허니팟과 비교하였다.

특징	기존 허니팟	악성코드 수집용 허니팟
운영체제	단일 운영체제	두개 이상의 운영체제
네트워크	단일 네트워크	두개 이상의 네트워크
가상화	필수조건은 아님	필수조건
피해 확산 방지	허니넷(Honeynet) 이용	자체 Outboud 트래픽차단
수집대상	시스템 로그	생성/변경된 파일
보안채널	필수조건은 아님	의심파일 전송용
감시대상	패킷	패킷, 파일 동작

표 1. 기존 허니팟과 악성코드 수집용 허니팟 비교

기존 허니팟과 달리 악성코드 수집용 허니팟은 악성코드 수집용 운영체제와 시스템 관리용 운영체제로 구분되어야 하며, 네트워크도 기존 허니팟과 달리 수집용 네트워크와 관리용 네트워크로 구분되어야 한다. 따라서, 이를 구분하기 위해 가상화 기술을 이용하여 수집용 시스템과 관리용 시스템이 별도로 구분된 것처럼 동작하도록 구성되어야 한다. 또한 악성코드의 침입으로 제 2차 감염이 발생할 것을 막기 위해 악성코드 수집용 허니팟은 방화벽(Firewall)을 이용하여 Outbound 트래픽을 차단한다. 하지만 기존 허니팟은 크래커가 실제 네트워크에서 활동하는 착각을 일으킬 수 있도록 확산 방지 기법 대신 허니넷을 구성하여, 허니넷 안에서만 활동 하도록 구성한다. 수집대상으로는 기존 허니팟은 공격기법 분석을 위해 시스템 로그를 수집하지만, 악성코드 수집용 허니팟은 악성코드 감염으로 생성된 파일이나, 변경된 파일을 시스템 로그와 함께 수집한다. 기존 허니팟은 특별한 정보를 제공하는 것이 없어 보안 채널이 필요없으나, 악성코드 수집용 허니팟은 위험한 악성코드를 전송하는 것이므로, 외부 누출로 인한 피해 방지를 위해 보안 채널이 필수적으로 구성되어야 한다. 또한, 기존 허니팟은 침입하는 패킷을 주로 감시하였으나, 악성코드 수집용 허니팟은 악성코드 행위를 알기 위해 패킷 뿐 아니라 파일 동작 및 프로세스 동작을 상세하게 감시하여야 한다.[13-14]

3.2.악성코드 수집용 허니팟의 7 대 요구조건

악성코드 수집용 허니팟은 기존 허니팟과 다른 다양한 특징들을 가지고 있으며, 이러한 특징들은 곧 악성코드 수집용 허니팟 구축시에 충족해야 할 요구사항이 된다. 따라서, 본 절에서는 악성코드 수집용 허니팟이 갖추어야할 7 대 요구조건을 아래와 같이 개발하였다.

①악성코드를 유도하기 위해 취약점을 내포해야 한다.
②악성코드 수집용 시스템과 허니팟 관리를 위한 시스템이 분리되어야 한다.
③악성코드 수집용 네트워크와 허니팟 관리용 네트워크가 분리되어야 한다.
④악성코드 감염으로 인한 피해 확산을 방지하는 기능을 제공해야 한다.
⑤악성코드 감염으로 인한 시스템 Freezing 방지 기능을 제공해야 한다.
⑤악성코드 의심파일을 전송하기 위한 보안 채널을 제공해야 한다.
⑥시스템에 침입하는 모든 패킷을 감시할 수 있어야한다.
⑦시스템을 침입한 악성코드 의심파일의 행위를 감시해야한다.

본 7 대 요구조건은 악성코드 수집을 위한 허니팟이 갖추어야 할 필수조건이며, 이 필수조건을 만족하도록 구축해야, 악성코드 수집 및 운영이 가능한 허니팟을 구축할 수 있다.

4. 악성코드 수집을 위한 허니팟 구현 모델

본 장에서는 악성코드 수집용 허니팟이 갖추어야 할 7 대 요구조건을 기반으로 독자적으로 개발한 악성코드 수집용 허니팟의 구현모델을 설명한다.

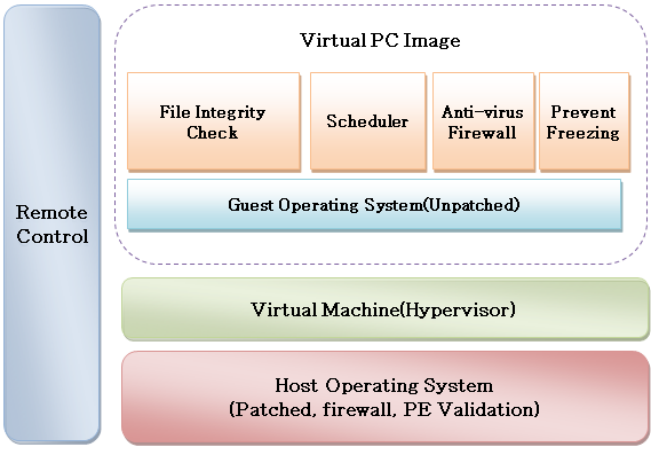

그림 1. 악성코드 수집용 허니팟 구현 모델

구현 모델의 구성요소를 살펴보면 다음과 같다.

표 2. 악성코드 수집용 허니팟의 구성요소

구성요소	특징	설명
Host System	Patched	취약점을 내포하지 않도록 보안패치가 완료된 상태
	Firewall	외부의 공격으로부터 보호를 위한 방화벽
	PE Validation Check	실행되는 파일인지를 체크하는 기능
Guest System	Non-patch	외부로부터 악성코드 침입을 유도하기 위해 취약점을 내포한 상태
VMM	Full Virtualization	Host OS 와 Guest OS 를 가상으로 구분하는 전가상화 기술
Management	File Integrity Check	Guest OS 상에서 변경된 파일을 찾기 위해 시스템을 무결성 체크하는 기능
	Scheduler	무결성 체크 등 각종 점검을 주기적으로 수행
	Anti-Virus	기 진단되는 악성코드를 제거하는 기능
	Firewall	Guest OS 에 침입한 악성코드의 공격이 외부로 나가지 않도록 차단하는 기능
	Prevent Freezing	악성코드에 의해 Guest OS 가 멈추는 것을 방지하는 기능
	Remote Control	원격에서 허니팟 시스템을 관리할 수 있는 원격관리 기능
	보안채널	악성코드 전송 시 암호화를 통한 전송 기능

표 2 의 허니팟 구현모델의 구성요소를 보면, Host Operating System 은 허니팟 시스템을 관리 하기 위한 용도로 사용되는 정상적인 시스템이어야 한다. 따라서, 보안패치(patch)가 되어 있어야 하며, 외부 공격으로부터 방어하기 위해 Firewall 이 구축되어야 한다. 또한 최종적으로 악성코드로 판단되는 파일을 전송하기 전에 해당 파일이 실행 가능한 파일인지를 체크하는 PE Validation Check 기능을 가지고 있어야 한다. 이는 대부분의 악성코드가 실행이 되어야 악의적인 기능을 하기 때문에, 기본적으로 악성코드는 실행되는 파일을 전제로 한다.(단, Script 와 같은 예외는 존재한다.) 또한 Guest Operating System 은 실제 악성코드를 수집하는 시스템으로써, 협의의 허니팟이다. 따라서, 허니팟은 취약점을 내포하고 있어야 함으로, 보안패치가 되지 않은 Unpatched 상태여야 한다. 또한 주기적으로 변경된 파일을 체크하여 악성코드로 의심되는 파일을 찾기 위해 File Integrity Check 기능을 Scheduling 을 통해 주기적으로 체크 해야 한다. 또한 기존에 진단되는 악성코드는 수집할 필요성이 없으므로, 수집 전에 진단하여 제거하기 위해 Anti-Virus Software 가 설치되어 있어야 하며, 감염된 Guest OS 에 침입한 악성코드에 의한 공격이 외부로 나가지 않도록 Firewall 이 Outbound 트래픽을 차단하여야 한다. 그와 함께 악성코드로 인한 시스템의 Freezing 증상을 방지하기 위해 Prevent Freezing 기능을 가지고 있어야 한다. 그 외에 수집된 악성코드를 중앙 샘플 수집 서버로 안전하게 전송하기 위해 암호화된 보안채널을 보유해야 한다. 허니팟은 보통 국내/외 원격지에 허니팟이 설치되기 때문에, Remote Control 을 설치해야 한다. 가장 중요한 구성요소로, Host OS 와 Guest OS 를 물리적으로 분리된 것처럼 구성하여, Host OS 위에 취약한 Guest OS 가 구성되도록 가상화하는 Virtual Machine 의 전가상화 기술인 VMM 이 탑재되어야 한다. 지금까지 악성코드 수집용 허니팟의 구현모델을 설명하였다. 실제 구현 시에는 운영 환경에 따라 구현 모델을 기반으로 적절한 기능을 추가 및 변경하여 구축하면 된다.

5.악성코드 수집용 허니팟 시스템 구현

본 장에서는 허니팟 구현 모델을 통해 구현한 실제 허니팟의 시스템, 네트워크, H/W, S/W 구성을 안내한다.

그림 2 는 악성코드 수집용 허니팟 내부의 구성도로써, 구현모델에서 제시한 Host System 과 Guest System 의 구성요소를 기반으로 구현 하였다.

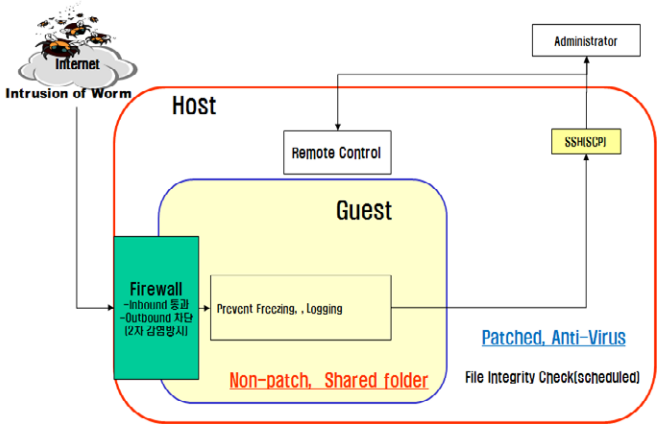

그림 2. 악성코드 수집용 허니팟 시스템 구성도

그림 3 은 악성코드 수집을 위한 허니팟 시스템의 네트워크 구성도로써, 허니팟 시스템은 샘플 수집용 네트워크를 통해 악성코드 의심파일을 수집하고, 관리용 네트워크를 수집된 의심파일을 전송함과 동시에 허니팟 모니터링 서버를 통해 시스템을 원격해서 관리 및 업데이트 하도록 구현하였다.

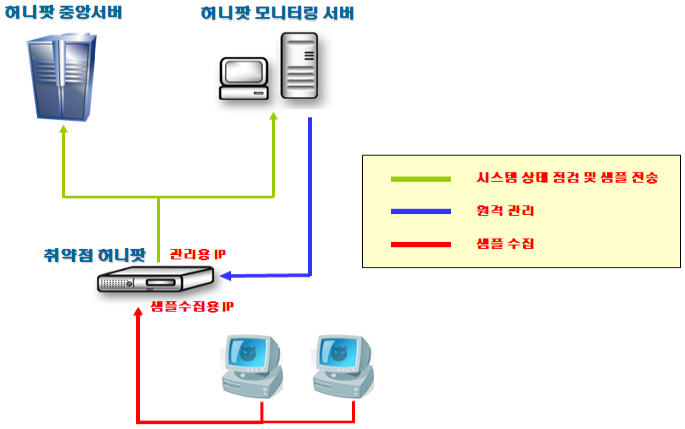

그림 3. 악성코드 수집용 허니팟 네트워크 구성도

표 3 은 악성코드 수집용 허니팟의 하드웨어, 소프트웨어 구성물로써, 허니팟 시스템을 구성하기 위한 권장 사양이다.

표 3. 악성코드 수집용 허니팟의 H/W, S/W 구성

H/W	Host System	- H/W . CPU 2.4G Hz . RAM 1G . HDD 80G -Lan(100/1000) X 2
S/W	Host System	- OS : Windows 2000 Professional - 시스템 보호 및 V3 진단 . AhnLab Security Pack - 원격관리 Agent
	Guest System	- OS : Windows 2000 Professional
N/W	- Host, Guest 용 네트웍크 IP · 2개	
기타	- 백업용 하드디스크 80G 1개(각 사이드당 한개만 있으면 됨)	

6. 악성코드 수집용 허니팟 시스템 구축 결과

본 장은 악성코드 수집용 허니팟 시스템을 국내,외에 설치하여 얻은 구축 결과와 함께 결과에 원인에 대한 분석한다.

표 4. 악성코드 수집용 허니팟의 설치 현황

설치 국가	설치 대수	설치 위치
한국	3 대	인터넷
	2 대	내부 네트워크
일본	1 대	인터넷
멕시코	1 대	인터넷
콜롬비아	1 대	인터넷
인도네시아	1 대	인터넷
대만	1 대	내부 네트워크
미국	1 대	내부 네트워크
계	11 대	인터넷 7 대, 내부 네트워크 3 대

국내에 5 대의 허니팟을 설치하였으며 이중 3 대는 샘플 수집을 위한 네트워크로 ADSL 을 이용하여 외부 인터넷과 직접 연결하였으며, 2 대는 내부 네트워크에 설치하였다. 해외는 총 6 대의 허니팟을 해당 국가별 ISP 망에 설치하였으며 이중 4 대는 DSL 계열 회선을 이용하여 외부 인터넷에 접속하였으며, 2 대는 내부 네트워크에 설치하였다.

표 5. 악성코드 수집용 허니팟의 의심파일 수집결과

설치 국가	수집 비율	설치 대수
국내	23.5%	5 대
해외	76.5%	6 대
설치 위치	**수집 개수**	**설치 대수**
인터넷	92.4%	7 대
내부 네트워크	7.6%	3 대

악성코드 수집용 허니팟을 이용하여 3 개월간 수집한 결과를 설치 국가면에서 보면, 국내에 설치된 허니팟에서 수집된 의심파일 개수는 전체 수집 개수의 23.5%, 해외는 76.5%로 파악되었다. 설치 위치로 구분하면, 인터넷에 직접 연결한 경우는 전체 수집 개수의 92.4%, 내부 네트워크 위치한 경우는 7.6%로 확인되었다. 수집 결과를 분석해보면, 설치 국가 측면에서는 국내보다는 국외에서 악성코드의 활동이 많은 것을 알 수 있었으며, 특히, 중남미, 동남아 국가의 악성코드 수집률이 상대적으로 타 국가보다 높은 것이 확인되었다. 이는 해당 국가의 보안 환경과 통신환경에 기인하는 것으로 보인다. 설치 위치면에서 보면, 내부 네트워크에 설치된 허니팟의 수집률이 낮았으며, 의심파일들이 1 차적으로 방화벽이나 IDS, IPS 를 통해 차단되어 내부로 침투하지 못한 것이 주요 이유로 보인다. 또한, 내부로 악성코드들이 침입하더라도 VLAN 등의 가상 네트워크 분리를 통해 활동 시에 네트워크 대역의 제약을 받아, 확산이 낮은 것으로 보인다.

7. 악성코드 수집용 허니팟 시스템 구축 시 고려사항

본 장에서는 수집결과를 통해 효과적인 악성코드 수집용 허니팟 시스템을 구축하기 위해서 고려해야 할 사항들은 제시한다.

①보안이 상대적으로 취약한 외부 네트워크 단에 허니팟 설치를 고려해야 한다.
②국내보다는 해외에서 악성코드 발생률이 높으므로, 해외 위주의 허니팟 시스템 구현을 고려해야 한다.
③해외에 허니팟 설치 시에는 해당 국가의 환경에 따라, 네트워크의 품질이 상이함으로, 사전에 국가별 제공되는 네트워크 품질을 고려해야 한다.
④VLAN 으로 네트워크 대역을 구분한 경우에는 내부 네트웍 단에 여러대의 허니팟의 설치를 고려하거나, IDS, IPS 에 탐지된 경우 허니팟으로 트래픽을 전환하는 방식을 고려해야 한다.

8. 결론 및 향후 연구계획

본 논문에서는 시스템에 대한 공격 방식이 크래커의 공격에서 악성코드를 이용한 공격으로 변화되면서, 악성코드 수집용 허니팟의 필요성이 크게 대두된 점에 주목하였다. 하지만, 기존 허니팟과 다른 특징을 가진 악성코드 수집용 허니팟을 개발할 때 구현모델이 없어 활성화 되지 못하는 문제점을 해결하고자 기존 허니팟과 다른 악성코드 수집용 허니팟이 갖추어야 할 7 대 요구조건을 개발하였다. 이 요구조건을 기반으로 허니팟을 구축 시 활용할 수 있는 구현 모델을 제안하였다. 또한, 구현 모델을 통해 실제 허니팟을 구현하였으며, 구성도와 사양 등을 통해 Anti-Virus 연구소에서 허니팟을 구축시 도움이 되도록 하였다. 실제 구현된 허니팟은 전세계적으로 7 개소 11 대가 설치되었으며, 이 결과를 통해 허니팟 설치시 고려해야 할 사항 등을 도출하였다.

본 논문에서 제시한 악성코드 수집용 허니팟 구현모델과 구현결과, 구현 시 고려사항을 통해 다수의 우수한 허니팟을 개발한다면, 악성코드를 조기에 수집 대응 함으로써, 1.25 대란, 7.7DDoS 대란과 같이 악성코드로 인해 발생하는 대규모의 국가적, 금전적 손실을 예방하는데 기여할 것으로 보인다.

향후 연구계획으로는 글로벌 허니팟 시스템을 구현한 결과를 통해 국내,외 정보통신 인프라 및 보안 환경 차이에 따른 구축모델을 세분화하는 연구를 진행할 계획이다. 또한, 취약점을 통한 허니팟 외에 이메일을 통해 전파되는 악성코드를 수집할 수 있는 이메일 웜 수집 허니팟, 웹 해킹을 통해 전파되는 악성코드를 수집하는 웹 허니팟 등 악성코드의 전파 경로에 맞게 다양한 허니팟 모델을 개발 및 구현하는 연구를 진행할 예정이다.

참고문헌

[1] 박찬호, 강권학, 권영찬, 장희진, 김철호, “메모리 감시를 이용한 허니팟 기반의 봇넷 역추적,” 한국정보과학회, 한국컴퓨터종합학술대회 논문집, pp.25-28, 2007년 6월.
[2] F. Freiling, T. Holz, and G. Wicherski, “Botnet Tracking-Exploring a Root-Cause Methodology,” ESORICS 2005, LNCS 3679, pp. 319-335, 2005.
[3] R, Puri, “Bots & Botnet: An Overview,” GSEC Practical Assignment Version1.4b, SANS Institure, Aug. 2003
[4] D. Barroso, “Botnets-The Silent Threat,” ENISA Position Paper, Nov. 2007.
[5] “Know Your Enemy Honeynets,” http://www.honeynet.org, 2006
[6]“Honeynets in Universities,” http://www.honeynet.org, 2004
[7] “ASEC Report 2009,” AhnLab Corporation, 2009
[8] 한국정보보호진흥원, 정보보호 포털 사이트, http://www.securenet.or.kr
[9] 이한우, 최현상, 이희조, “DNS 기반의 봇넷 탐지 시스템,” 한국정보처리학회 추계학술발표대회논문집, pp. 13790-1382, 2006 년 10 월
[10] 최효식, “꿀단지 네트워크, 허니팟” 마이크로소프트웨어, pp. 209-215, 2005 년 6 월.
[11] 김영화, “미래인터넷의 네트워크 가상화 기술 동향,” ETRI 전자통신동향분석 제 25 권 1 호, 2010
[12] 허종오, “ACCESS Control,” 한국생산성본부 CISSP Foundation, 2009
[13] 허종오, “AhnLab Global Honeypot, ”안철수연구소, 2009
[14] http:// www.ahnlab.com.