제로데이 어택 방지를 위한 실시간 대응기술

오 진 태* 장 종 수** 류 재 철***

목 차

1. 서 론

정보기술의 발전으로 오늘날 초고속 인터넷 사용이 일반화되어 네트워크 트래픽 양이 현저하게 증가되고 있다. 또한 발달된 네트워크 인프라를 활용한 다양한 IT 서비스가 개발되어 사용자들이 더욱 편리한 생활을 할 수 있게 되었다. 이러한 네트워크 인프라 발전과 함께 프로세서 기술의 발전으로 인한 고성능 PC로 인해 더욱 많은 양의 데이터를 단시간에 처리할 수 있게 되었다. 하지만 인터넷의 특성인 개방망 환경으로 인한 해킹, 바이러스 유포, 지적 재산권의 침해, 사이버 범죄에 이용되는 등과 같은 정보화 역기능으로 인하여 개인의 사생활 정보 유출은 물론 국가 안보까지 위협받는 상황에 이르렀다. 이러한 위협은 1차적으로는 악성코드에 의해 유발된다고 할 수 있다.

수년 전까지 해커들은 악성 코드를 전파하기 위해 네트워크에서 취약한 시스템을 자동으로 찾고 악성코드를 전파하여 단시간에 많은 호스트를 감염시키는 방법을 사용하였다. 하지만 이러한 자동 전파 기법은 네트워크 트래픽 분석으로 쉽게 공격이 탐지되므로 공격 횟수가 줄어 들고 있는 실정이다. 현재는 해커들이 서버를 해킹하고 해킹된 홈페이지를 방문하는 사용자가 자동으로 악성 코드를 다운 받도록 링크를 걸어두는 기법이 일반화되고 있어 악성 코드를 탐지하기 더욱 어려워졌다. 또한 최근에는 다양한 해킹 기법들이 결합되고 있으며 인터넷을 통해 너무나 쉽게 해킹 툴들을 얻을 수 있게 되어 대응이 더욱 힘들어 지고 있다. 개인 PC로 악성코드가 유입되는 것은 1차적인 피해로 보아야 한다. 이로 인해 2차적으로 발생하는 DDoS, 개인정보 유출 등의 문제가 지속적으로 발생하고 있으며, 이를 해결하기 위한 다양한 대응 방법들이 연구되고 있다. 현재 사회적으로 문제가 되고 있는 사이버 공격은 주로 2차 피해에 속하는 DDoS나 개인정보 유출이라는 현상을 해결하기 위한 방법에 초점이 맞추어져 있다. 하지만 해킹 문제를 근본적으로 해결하기 위해서는 악성 코드가 PC로 유입되는 1차 단계에 대한 대응 기술이 필요하다. 취약점이 발표되고 이에 대한 패치가 나오기 전까지 발생하는 모든 공격을 Zero-day 공격이라 한다. 이러한 공격의 경우 패치가 적용되지 않은 많은 시스템들이 공격의 대상이 되므로 막대한 피해가 예상되며, 해당 공격을 탐지하기 위한 시그니처도 갖고 있지 않아 더욱 위험한 공격이다. 일반적으로 공격 코드는 실행 가능한 코드가 대부분이므로 zero-day 공격을 탐지하기 위해 악성코드를 탐지 하는 기술이 필요하다. 본고에서는 네트워크 단에서 실행 가능한 모든 파일을 재조합하고 이들의 악성 여부를 탐지하고 대응하는 기술에 대해 논하고자 한다. 2장에서는 기존의 악성 코드 탐지 기법에 대해 간략히 알아본다. 3 장에서는 네트워크 상의

* 한국전자통신연구원 보안게이트웨이연구팀
** 한국전자통신연구원 정보보호연구본부
*** 충남대학교 정보통신공학부

Zero-day 공격과 악성 코드 탐지 기능을 구현한 ZASMIN (Zero-day Arrack Signature Management Infrastructure) 시스템에 대해 간략하게 정리하고, 4장에서는 ZASMIN 시스템을 Reference site에서의 운용한 결과를 정리하고, 5장에서 결론을 내리고자 한다.

2. 관련 연구

Zero-day 공격을 탐지하기 위한 기법들은 네트워크 레벨의 접근과 호스트 기반의 접근으로 분류된다. 네트워크 패킷들에서 반복된 패턴을 찾아내고 공격 시그니처를 생성하는 Earlybird가 있다.[1] 이 기법은 웜의 특성을 이용하여 네트워크에서 자주 발생되는 content를 Rabin Fingerprint 기법을 이용하여 찾아내고 해당 컨텐츠를 포함한 패킷들의 단위 시간 동안 얼마나 많은 호스트로 전달되었는지의 여부에 따라 시그니처를 생성하지만, 생성된 시그니처가 공격과 연관성이 떨어져 오탐율이 높고 단순한 다형화 공격에도 취약하다.

Autograph/polygraph의 경우도 웜 등 악성 코드의 경우, 공통된 패이로드를 가지고 있다는 특성을 이용하여 시그니처를 생성한다.[2][3] 이 기법은 Earlybird에 비해 다형화 공격에 대해 좀더 정확한 시그니처를 생성하지만, 여전히 공격과 연관성이 떨어지는 시그니처를 생성하는 단점을 지니고 있다.

인터넷 서비스의 특성에 따라 실행 가능한 코드가 전달 될 수 없다는 특성을 이용하여 악성 코드를 탐지 하는 방법인 Sigfree 기법이 있다.[4] 이 기법은 윈도우 기반의 플랫폼에서 제공되는 Web 서비스 (port 80), Remote Access Services (port 111,137,138,139), MS-SQL service (port 1434), Workstation services (port 139, 445) 등은 정상적인 패킷에는 실행 코드를 포함하지 않고 있지만, 버퍼 오버플로우 공격의 경우 실행 가능한 코드를 포함하는 패킷을 전달하는 특성을 활용하여 공격을 탐지한다. 하지만 이 기법은 정상적인 서비스는 실행 가능한 코드를 포함하고 있지 않다는 가정을 전제로 하는 서비스에서만 해당된다. 또한 패킷을 재 조합하지 않고 단지 패킷 단위의 분석만 수행하며, SQL Injection 등의 응용 계층 공격은 탐지 대상에서 제외된다는 단점이 있다.

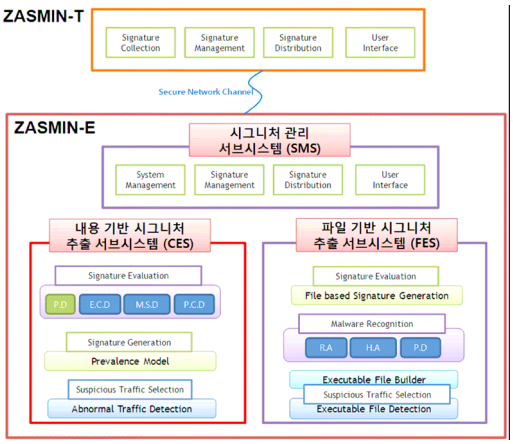
비정상적인 패이로드 분포를 분석하여 공격을 찾아내는 Payl 기법이 있다.[5] 이 기법은 특정 사이트로 입력되는 비정상 패이로드와 입력시 사용된 동일한 포트로 출력되는 패킷의 상관 관계를 이용하여 공격을 탐지하는 기법이다. 이러한 분석이 가능한 이유는 웜의 경우 내부의 호스트를 감염시키면 감염된 호스트가 다른 호스트를 감염시키기 위해 웜을 발생하는 특성을 이용하여 악성 코드를 탐지하는 것이다. 이 기법에서 비정상적인 패이로드를 찾기 위해 정상적인 패킷들의 N-gram을 이용한 분석 값을 계산하고 네트워크로 입력되는 패킷들의 패이로드에서 N-gram을 계산한 후 이들의 상관관계를 Mahalanobis distance를 이용하여 특정 임계치를 초과는 경우 비정상 패이로드로 선정하고 이들이 네트워크 내부에서 다시 전파되는지 확인하는 방법으로 공격을 찾아낸다. 이 기법은 자동 전파력을 가진 웜 등의 탐지가 쉬운 장점이 있으나, 홈페이지 변조 등을 통해 직접 전달된 악성 코드를 탐지하지 못하고, 초기 정상 패이로드를 어떻게 선정하는가에 따라 탐지 결과가 달라 질 수 있다는 단점이 있다.

다음으로는 웜의 경우 자기 코드를 수행하기 위해 주소 점프를 해야 하는데 이 때 점프 하는 주소를 임의로 변경하여 웜이 작동하지 못하게 하는 Packet Vaccine 기법이 있다.[6] 이 기법은 호스트 단에서 새로운 악성코드가 동작되지 못하도록 할 수는 있지만 잘못된 주소 점프에 의해 세그먼트 폴트나 Illegal Instruction Fault 등이 발생할 가능성이 있다.

마지막으로 호스트 기반에서 외부에서 유입된 모든 코드를 Taint tracking에 의해 시스템 내부의 권한을 획득하는 지를 찾고 직접 코드를 자동 분석하는 MINOS/ DACODA 기법이 있다.[7][8] 이 기법은 허니넷으로 유도된 코드가 어떠한 악성행위를 하는지를 분석하는 기법으로 인터넷 사용자들이 변조된 홈 페이지 등을 방문하고 악성코드를 다운로드 받는 등의 경우 악성코드가 허니넷으로 유도되지 않는 예와 같이 허니넷을 유도되지 않는 코드는 분석이 불가능하다. 이 기법은 본 연구원에서 개발하고 있는 시스템에서 수집한 악성 코드를 분석하기 위한 방법으로 적용되기 위해 국제 공동연구를 진행되었다.

3. ZASMIN 시스템 구조

본 연구원에서는 알려지지 않은 공격을 효과적으로 대응하기 위해 ZASMIN을 개발하였다. 이 시스템은 고속으로 전파되는 슈퍼 웜 형태의 이상 공격뿐만 아니라, 네트워크를 통한 악성코드(malware)전파를 탐지하고 대응할 수 있는 시그니처를 실시간으로 생성하여 해당 공격에 의한 피해를 최소화할 수 있는 시스템이다. ZASMIN은 ZASMIN-Endpoint(ZASMIN-E) 시스템과 ZASMIN-Top(ZASMIN-T) 시스템으로 구성된다. ZASMIN-E 는 네트워크에서 이상 트래픽 및 악성코드를 탐지하고 이들에 대한 시그니처 자동 추출하고, ZASMIN-T는 여러 대의 ZASMIN-E에서 생성된 시그니처를 관리한다. ZAMIN-E는 이상 트래픽을 탐지하기 위해 내용 기반으로 시그니처를 추출하는 CES(Contents based signature Extraction Sub-system), 악성 코드를 탐지하기 위한 파일 기반 시그니처 추출하는 FES(File based signature Extraction Sub-system), 생성된 Signature를 관리 분배하는 SMS(Signature Management System)의 3개 서브시스템으로 구성된다.



(그림 1) ZASMIN 구조

3.1. 내용 기반 시그니처 추출 서브 시스템 (CES)

내용기반 시그니처 추출 서브 시스템은 네트워크에 유입되는 트래픽을 모니터링하여 이상 트래픽을 찾아내는 이상 트래픽 탐지 기능, 이상 트래픽의 패킷에 공격과 관련된 특징이 포함되어 있는지를 조사하여 공격 탐지 시그니처를 자동 생성하는 시그니처 생성 기능, 생성된 시그니처를 평가하는 시그니처 기능블록으로 구성된다.

CES는 이상 트래픽 탐지에 사용될 트래픽 정보를 생성하기 위해 2 Gbps 선로 속도를 갖는 하드웨어가속 보드를 사용한다. 하드웨어는 트래픽 용량별 정보, 세션관련 정보, 목적지 주소별 정보 등을 수집하는데, 최소 단위 흐름(Primitive Flow)과 집합 흐름(Aggregation Flow)인 2종류의 트래픽을 수집한다. 첫째, 최소단위 흐름은 micro 분석에 사용되며, 패킷의 IP 헤더에 있는 근원지 IP 주소, 목적지 IP 주소, 프로토콜, 포트로 구분된다. 둘째, 집합 흐름은 이상 트래픽 근원지를 찾아내기 위해 사용되며, 근원지 IP 주소, 포트와 프로토콜 기준으로 분류되는 흐름과 목적지 IP 주소와 프로토콜 기준으로 분류되는 흐름으로 구성된다.

시그니처 생성 기능은 이상 행위 트래픽으로 분류되는 것에 대해 해당 패킷에 대한 시그니처를 생성하고, 시그니처 생성에 사용된 패킷들에서 공격 관련 행위가 있는지 확인하는 공격 연관성 분석을 한다. 이 기능은 연관성 분석을 위해 패킷 내의 Contents 분석 기능과 Binary Data 분석 기능으로 이루어진다. Packet Contents 분석 기능은 하드웨어로부터 전달받은 네트워크 패킷을 이용하여 해당 패킷의 Payload부분에 공격의 특징이 포함되어 있는지를 분석하여 해당 네트워크 패킷이 공격의 일부인지를 판단한다. Binary Data 분석 기능은 하드웨어로부터 전달받은 네트워크 패킷을 이용하여 해당 패킷의 Binary Data를 분석하여 해당 네트워크 패킷이 공격의 일부인지를 판단한다.

시그니처 평가기능은 공격코드를 다형화하였는지의 여부를 검사하는 P. D. (Polymorphic Detection)검사를 수행하여 다형화된 공격 코드까지 찾아내도록 되어 있다. 또한 E.C.D.는 실행 가능한 코드를 찾는 기능으로 공격 코드와 일반 데이트를 역 리어셈블 할 때 발생하는 스팩터럼의 차이를 이용하는 등의 방법을 활용하여 실행가능 코드 포함여부를 확인하고 있다. 또한 M.S.D.는 악의적인 스트링 포함 여부를 확인하는 기능이며, P.C.D.는 프로토콜의 특성을 활용하여 공격 가능성을 판단 하는 기능이다. 이상 시그니처 평가는 다양

한 검사 기능을 적용하여 시그니처와 공격 연관성을 분석하므로 실제 생성된 시그니처가 공격과 연관성이 매우 높은 시그니처가 생성 될 수 있도록 하고 있다.

3.2. 파일 기반 시그니처 추출 서브 시스템 (FES)

FES는 파일 추출 기능, 파일 재조합 기능, 악성 코드 분석 기능, 시그니처 생성과 평가 기능블록으로 구성된다. 파일 기반 시그니처를 추출하기 위해 네트워크으로 전달되는 모든 실행 가능 파일과 관련된 일련의 패킷들을 실시간으로 수집하여 CPU로 전달하는 기능을 하드웨어가 수행한다. 이를 위해 하드웨어에서는 실행 가능 파일 가능성이 있는 일련의 패킷들을 인식하기 위하여 고속 패턴 매칭 기능과 세션 관리 기능을 수행한다.

파일 재조합 기능은 CPU로 전달된 실행가능 파일과 관련된 일련 패킷들에 대하여 실행 가능한 형태의 파일형식으로 재 조합한다.

악성코드 분석 기능은 재 조합된 실행 가능 파일은 헤더 분석 기능, 비정상 영역 탐지 기능, 팩(Pack) 탐지 기능을 적용하여 악성 코드인지를 분석한다. 헤더 분석 기능은 실행 가능 파일의 헤더 분석을 통하여 악성 코드가 가지는 전형적인 특성을 탐지하는 기능을 수행한다. 비정상 영역 탐지 기능은 실행 가능 파일의 영역 별 특성 분석을 통하여 비정상 실행 파일을 탐지하는 기능을 수행한다. 마지막으로 팩 (packed) 탐지 기능은 악성 코드의 특성 중 하나인 실행 형 PACKED 코드 탐지를 통하여 악성 유무를 판단하는 기능을 수행한다. 이상의 분석 방법에 의해 분석된 결과들은 악성 코드 특징과 공격 가능성을 정량적 수치로 표기하여 파일 기반의 시그니처 생성 기능으로 전달한다.

시그니처 생성 기능은 악성 코드로 판정된 파일 내에 존재하는 특징을 기반으로 해당 패킷을 탐지해 낼 수 있는 시그니처를 생성하는 기능과 악성 코드 유무 결과를 토대로 각 방법에 가중치를 부여하여 해당 결과를 산출하는 역할을 수행하며, 산출된 평가 결과를 Certificate형태로 구성하여 시그니처 관리 서브시스템으로 전달하는 기능을 수행한다. 추출된 시그니처는 해당 세션의 정보와 함께 SNORT의 시그니처 구문 형식으로 생성된다.

4. ZASMIN의 Reference Site 운용 결과 분석

ZASMIN은 현재 기업망 백본, 국내 4대 관문국중 한 곳의 허니넷, 서버팜, 대학 캠퍼스 네트워크등 4개의 Reference Site에서 시험 운용 중이다. ZASMIN은 설치된 망의 특성에 따라 다른 운용 결과를 보여 주고 있다.

이용자들이 많은 기업망과 캠퍼스 망의 경우 실행 가능한 코드의 유입이 많았으며, 이들 중 1~3%정도는 악성으로 탐지되었다. 평균 600Mbps, 최대 1Gbps의 트래픽 환경을 가진 기업망에서 운용중인 ZASMIN의 GUI 화면은 그림 2와 같다.

(그림 2) ZASMIN 운용 화면

하지만 서버팜에 운용중인 ZASMIN의 결과를 보면 실행 가능한 코드의 유입이 적은 것으로 확인되었다. 이러한 사실은 현재 악성코드의 유입이 사용자들이 인터넷을 통하여 다양한 호스트에 접속하면서 감염된 호스트로부터 실행 가능한 다양한 코드들이 유입되는 현상으로 설명할 수 있다.

또한 허니넷의 경우 유입되는 트래픽이 평균 수백 Kbps에 불가하지만 유도된 트래픽의 대부분이 공격 트래픽일 가능성이 높다는 특성을 가지고 있다. 각 사이트의 ZASMIN 운용 결과는 표 1과 같다.

(표 1) Reference Site 운영 결과

구분		허니넷	기업망	서버팜	캠퍼스
CES	Alert 수	1,802	1,683	8,628	6,825
	시그니처 수	10	3	0	1
FES	수집 파일 수	3,897	34,707	9,976	14,057
	악성 파일 수 (ZASMIN /백신)	566 /210	589 /158	78 /0	194 /23

기업망에 설치된 ZASMIN의 경우 2008년 8월 첫 1주 동안 운영 결과를 분석하였다. 이기간 동안 기업망 외부 IP에서 기업 내부 PC들의 취약점 스케닝을 시도한 공격 행위는 1,683번 탐지 되었지만, 공격 코드가 유입되어 ZASMIN에서 시그니처를 생성한 경우는 3번에 불과했다. ZASMIN은 단순한 스캐닝 공격에 대해서는 로그만 발생하며, 스캐닝 시도와 함께 공격과 연관된 행위 예를 들어 패킷에 공격코드를 포함하거나, 포함된 공격코드의 시그니처 생성을 방해하기 위한 Polymorphic 코드가 있는 경우 등 8가지의 연관성 분석을 통해 공격으로 최종 판정되는 경우에만 시그니처를 생성하도록 설계되어있다. 스캐닝을 통한 공격으로부터 시그니처가 생성된 것이 적은 이유는 대부분의 스캐닝이 방화벽의 접근 차단 port 리스트에 의해 차단 당하여 기업 망 내부의 취약점을 가진 호스트로 전달되지 못하여, 취약점 스캐닝에 반응한 PC들이 수가 적어 공격 코드가 유입되는 단계까지 도달하지 못한 이유인 것으로 설명할 수 있다. 이러한 결과는 기존의 정보보호 제품들로 무장된 기업망이나 캠퍼스망의 경우 스캐닝을 통해 악성코드를 전파하는 기존의 악성코드 전파 방식은 네트워크 보안 장치에 의해 쉽게 탐지/차단되고 있어 공격 성공 확률이 줄어들고 있는 현실과 일치한다.

하지만 이 기간 동안 해당 기업망으로 유입된 실행 가능한 코드는 무려 34,707개나 ZASMIN에서 재조합 되었다. 이들 중 589개는 악성 코드일 가능성이 있는 것으로 ZASMIN이 분류 하였으며 이중 158개의 파일은 3개의 대표적인 상용 Anti-virus 제품으로 악성 코드임이 확인할 수 있었다. 또한 악성 코드의 대부분이 트로이 목마, IRC-Bot, Back Door 프로그램 등인 것으로 확인되었다. 이 중 IRC-Bot의 경우 악성코드로 인하여 감염된 PC들이 DDoS 공격지로 악용될 가능성이 있으며, Back Door 프로그램이나 트로이 목마에 감염된 PC의 자료들이 유출되는 등의 2차 피해가 예상되는 악성 코드임을 알 수 있었다. 이러한 현상은 캠퍼스 망도 비슷한 결과를 보여 주고 있다.

표 1에서 서버 팜에 설치된 ZASMIN의 경우 평균 트래픽은 800Mbps에 이르지만 재조합된 실행코드는 9,976개로 트래픽 량에 비해 현저히 적은 실행 코드가 재조합 되었으며, 악성으로 분류된 코드도 소량인 것을 확인 할 수 있었다. 또한 악성으로 분류된 코드의 대부분이 Adware 등으로 기업망이나 캠퍼스 망에서 볼 수 있었던 트로이 목마, IRC-Bot, Back-door 등의 악성코드는 확인되지 않았다.

위의 운영 결과에서 우리들은 기업망과 캠퍼스 망의 경우와 같이 사용자들이 인터넷을 통해 다양한 서버에 접속하면서 다량의 실행코드가 유입되고 있으며, 이들 실행 코드 중 1~3%는 ZASMIN에서 악성코드로 분류되고 있다. 또한 이들 중 30~40% 이상이 상용 백신 프로그램들에서도 악성코드로 탐지되는 공격인 것으로 확인 할 수 있었다.

ZASMIN에서 수집된 실행 코드를 3개의 상용 백신 프로그램으로 검사하여 적어도 하나의 백신에서 악성코드로 탐지된 코드에 대하여 중복되지 않은 악성 코드는 98개로 분류 되었다. 탐지 결과 최고로 많은 공격을 탐지한 백신은 80개의 공격을 탐지하였으며, 최소는 36개의 악성코드를 탐지 하는 결과를 보여 주었다. 사용자의 PC에 여러 개의 백신들을 인스톨하는 경우 서로 다른 백신들을 악성코드로 탐지하는 결과를 가져오기 때문에 많은 백신을 하나의 PC에 인스톨 할 수 없다. 또한 많은 백신을 인스톨 한다 하더라도 비용 문제가 발생하므로 해당 기업이 사용하지 않는 백신을 탐지할 수 있는 악성 코드의 경우 해당 기업의 망에서는 대응 할 수 없는 악성 코드로 분류되는 것이 더욱 심각한 문제라고 할 수 있다. ZAMSIN이 설치된 망들뿐만 아니라 대부분의 망들에서 기존의 해킹에 대한 대응은 철저한 반면 악성 코드 유입에는 네트워크에서 그 유입을 볼 수도 없으며, 기업망의 사용자들이 신고 하기 전에는 악성 코드 감염 여부도 알 수 없다는 문제를 지니고 있는 것으로 볼 수 있다.

사용자들이 정상적인 프로토콜을 사용하여 다양한

컴퓨터들을 접속하므로 정상적인 프로토콜을 통한 악성코드의 유입이 많은 양상을 보이고 있다. 하지만 현재까지 정상적인 프로토콜에 포함되어 유입되는 악성코드를 네트워크 단에서 모니터 할 수 있는 기술이 없었으며, 사용자의 PC들이 악성코드의 공격을 받아 비정상적인 행위를 하는 경우에만 이러한 공격 행위를 알 수 있었다.

5. 결 론

4장에서 네트워크 상의 악성 코드를 탐지해 내기 위한 새로운 기법과 이를 네트워크에 적용한 운용 결과와 이에 대한 분석을 해 보았다. 과거 공격자나 감염된 컴퓨터가 대량의 스캐닝을 통한 취약점을 자동을 찾아내고 악성코드를 유포하는 방법의 공격 회수는 감소 하고 있다. 이러한 공격은 대량의 트래픽 발생이 수반되므로 트래픽 분석을 통해서 비교적 쉽게 공격을 찾을 수 있었다. 하지만 현재 악성코드 유포를 위해 이미 악성코드에 감염된 호스트를 활용하고 있다. 사용자들이 이러한 서버를 접속하는 경우 악성코드가 자동으로 다운로드 되는데, 이러한 악성코드 다운로드는 대량 트래픽이 발생하지도 않으며, 정상적인 프로토콜을 사용하므로 악성코드 유입을 탐지하기 더욱 어려워 졌다. 본 논문에서는 이렇게 네트워크 패킷에 포함되어 있는 실행 코드들을 네트워크 상에서 재조합하고 이들의 악성여부를 자동으로 판단해 주는 ZASMIN 시스템에 대해 기술하였다. 또한 ZASMIN에는 재 조합된 모든 악성 코드를 보관하고 있어 상용 백신 등으로 이들이 어떠한 악성 코드인지 쉽게 알 수 있다. 현재 ZASMIN 시스템은 5곳의 Reference Site에서 성공적으로 운용 중이며 상용백신들로 검사해본 결과 다량의 트로이 목마, Bot, Back Door 등의 악성코드가 유입되는 것으로 확인되었다. ZASMIN을 활용하면 기업망이나 캠퍼스 망 등에서 현재까지 확인 할 수 없었던 악성코드 유입을 관제할 수 있을 것이며, 악성 코드 유입을 확인한 이후에는 이들 악성 코드 유입을 차단하고 대응할 수 있는 시스템이 개발될 것으로 기대한다. 현재 개발된 기술은 네트워크 상의 실행 가능한 코드만을 재조합하고 이들의 악성 여부를 판단하는 기술이 개발되었으나, 앞으로 Active-X, 첨부파일, Encoding 되거나 Zip등으로 압축된 파일에 대한 검사 기능이 개발되어야 할 것으로 보고 있다.

참 고 문 헌

[1] S. Singh, C. Estan, G. Varghese, and S. Savage. Automated worm fingerprinting. In OSDI, 2004.

[2] H.-A. Kim and B. Karp. Autograph: Toward automated, distributed worm signature detection. In USENIX Security Symposium, pages 271-286, 2004.

[3] J. Newsome, B. Karp, and D. Song. Polygraph: Automatically generating signatures for polymorphic worms. In Proceedings of the IEEE Symposium on Security and Privacy, May, 2005.

[4] SigFree: A Signature-free Buffer Overflow Attack Blocker, Usenix security 2006

[5] K. Wang, G. Cretu, and S. J. Stolfo. Anomalous payload-based worm detection and signature generation. In Proceedings of the 14th Usenix Security Symposium, Baltimore, MD, USA, July 31 – August 5 2005.

[6] XiaoFeng Wang, Zhuowei Li, Jun Xu, Michael K. Reiter, Chongkyung Kil, Jong Youl Choi1, Packet Vaccine: Black-box Exploit Detection and Signature Generation, CCS 2006

[7] Jedidiah R. Crandall and Frederic T. Chong, Minos: Control Data Attack Prevention Orthogonal to Memory Model, IEEE/ACM international symposium on micro-architecture, 221-232, IEEE Computer Society. 2004

[8] J. R. Crandall, Z. Su, S. F. Wu, and F. T. Chong. On Deriving Unknown Vulnerabilities from Zero-Day Polymorphic and Metamorphic Worm Exploits. ACM CCS, pages 235 – 248, November 2005

◐ 저 자 소 개 ◑

오 진 태

1990년 경북대학교 전자공학과 공학사
1992년 경북대학교 전자공학과 석사
1998년 한국전자통신연구원 선임연구원
1999년 MinMax Tech. 연구원
2001년 Engedi Networks Inc. Director
2003년 Winnow Networks Inc. CTO, 부사장, Cofounder
2003년~현재 한국전자통신연구원 보안게이트웨이연구팀장

장 종 수

1984년 경북대학교 전자공학과학사
1986년 경북대학교 대학원 전자공학과 석사
2000년 충북대학교 대학원 컴퓨터공학과 박사
1989년 7월~현재 한국전자통신연구원 정보보호연구본부 책임연구원
2008년 1월 ~ 현재 한국정보보호학회 부회장

류 재 철

1988년 5월 Iowa State University 전산학과 석사
1990년 12월 Northwestern University 전산학과 박사
1991년~현재 충남대학교 정보통신공학부 교수
1997년~현재 한국정보보호학회 이사
2001년~현재 국가정보원 정보보호시스템 인증위원회 위원
2003년~현재 인터넷침해대응기술연구센터장