신종 사이버 공격 탐지 및 차단을 위한 인프라 구축 프로젝트 (NoAH 와 ZASMIN 프로젝트)

김대원* 김익균** 오진태*** 장종수**** 조현숙*****

우리는 최근 몇 년 동안 바이러스, 웜, 트로이얀, 스파이웨어와 같은 사이버 공격들이 인터넷 상에서 점점 증가하고 있음을 목격해 왔다. 이런 사이버 공격들은 인터넷 사용의 효율성을 저해하고 있고, 수 분내로 대규모 네트워크 망을 전복시킬 정도로 IT 인프라의 위협이 되고 있다. 기존의 보안 시스템 및 인프라들은 알려지지 않은 새로운 사이버 공격들에 대해 사람의 분석을 통한 대응을 해 왔다. 그러나, 이런 방식은 즉각적인 대응이 필요한 상황에서는 종종 그 효율성이 떨어지기 때문에 공격 탐지와 대응을 위한 자동화된 방식에 대한 연구가 중요한 이슈가 되었다. 본 고에서는 알려지지 않은 신종 사이버 공격을 탐지하고 차단하기 위한 인프라 구축에 대한 최근의 대규모 프로젝트들을 소개하려고 한다. ▨

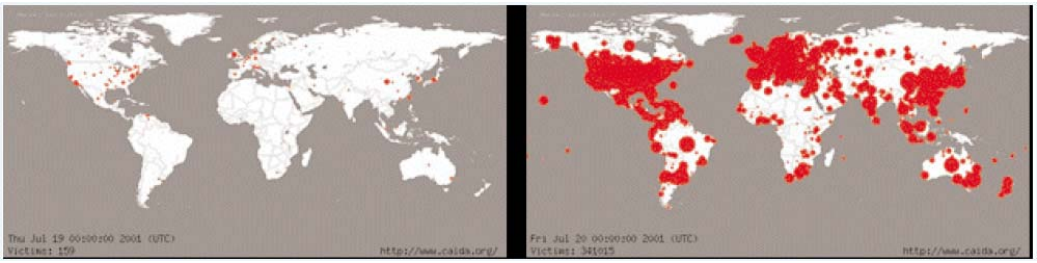
목 차

* ETRI 보안게이트웨이연구팀/연구원
** ETRI 보안게이트웨이연구팀/선임연구원
*** ETRI 보안게이트웨이연구팀/팀장
**** ETRI 보안게이트웨이연구팀/책임연구원
***** ETRI 정보보호연구본부/본부장

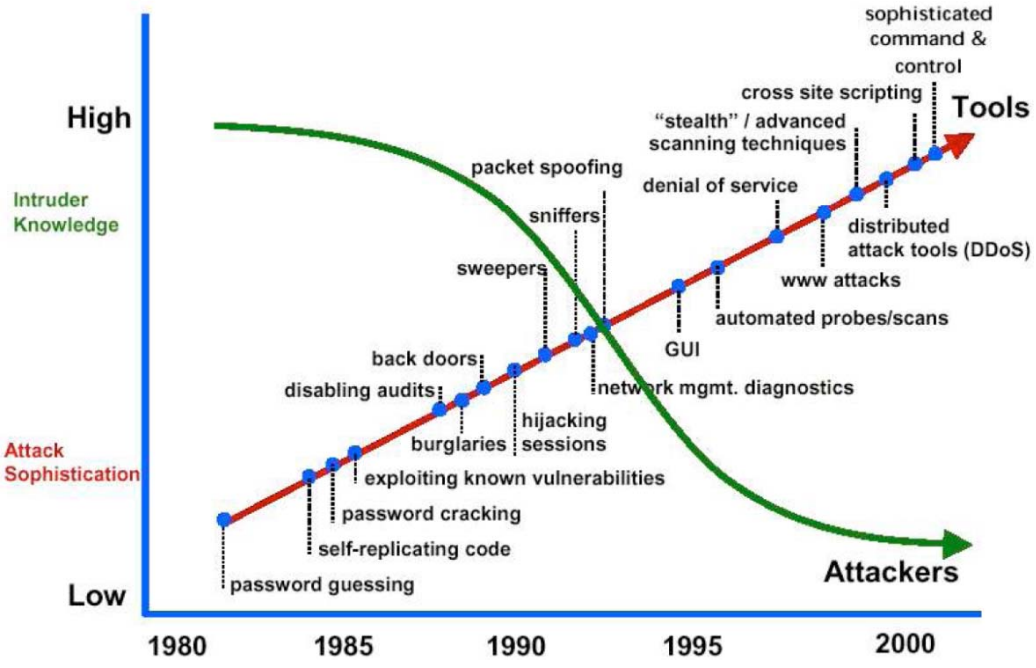
Ⅰ. 서 론

과거 수년 동안 우리는 대규모 웹 사이트부터 일반적인 가정용 컴퓨터와 최근의 모바일 기기까지 컴퓨팅 환경들을 위협하는 다양한 사이버 공격들의 증가를 목격해 왔다. 코드레드(Code Red) 인터넷 웜이 2001 년 발생했을 때, 전 세계적으로 수십 만대의 웹 서버들이 단지 수 일 내에 무력화 되었으며 그로 인해 심각한 사회적, 경제적 장애를 발생시킨 바가 있음을 모두 기억하고 있을 것이다[1]. 그 동안 산업계 및 학계뿐만 아니라 일반인들까지 사이버 공격에 대한 인식이 높아지고 중요한 노력들을 기울

여 왔음에도 불구하고, 우리는 여전히 사이버 공격에 노출되어 있으며 점점 그 양상이 지능화되고 있음을 확인하고 있다. 이 것은 사이버 공격의 발전이 혁신적[2]이라면, 보안 시스템의 발전은 그에 반해 더디게 진행되기 때문이다.

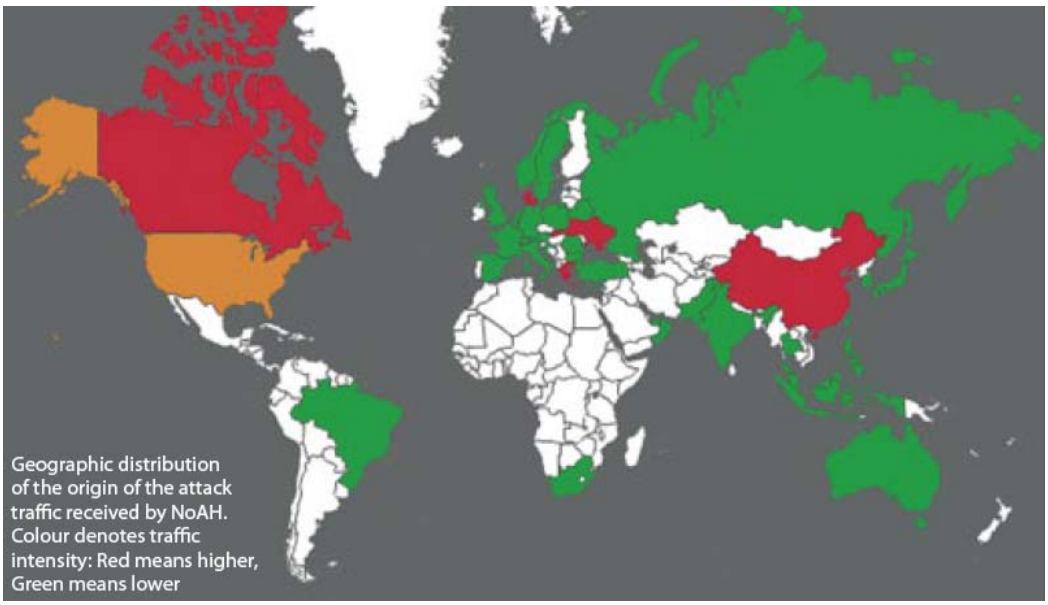


(그림 1) 24 시간 동안 코드레드에 의해 감염된 PC 의 확산 현황. 2001 년 7 월 19 일 감염된 PC 는 159 대였으나 (왼쪽), 7 월 20 일에는 341,015 대로 급속히 늘어났다. (오른쪽)



(그림 2) 사이버 공격 기법의 발전 현황 및 공격자의 지식 수준

사이버 공격은 그 규모, 복잡함, 확산속도 면에서 증가하는 양상을 띄고 있다. 일반인이 재미로 시작했을 수도 있고 유명세를 타기 위해 시작했을 수도 있지만, 그런 공격자들이 증가하고 있는 것이 사실이며, SPAM 메일, 자동 전파 웜 등에 의해 확산된 악성 프로그램들[3]이 언제 다시 분산 서비스 공격(DDoS Attack, Distributed Denial of Service Attack) 같은 악의적인 행위를 시도할 지 모르는 것이다.



(그림 3) NoAH에 의해 탐지된 사이버 공격 근원지의 지리학적 분포도. 적색이 높고, 녹색이 낮다.

우리는 점점 빨라지고 있는 인터넷 속도와 소프트웨어에 항상 존재할 수 있는 취약점으로 인해, 정보 인프라를 대상으로 한 빠르고 광범위하며 조직적인 공격들로 인한 사이버 공격들의 파괴력을 경험하였다. 이런 사이버 공격들에 대처하기 위해서는 확산되어 나가는 공격들만큼 빠르게 반응할 수 있는 자동화된 차단 시스템들을 필요하다. 현재의 방법들은 사람의 수작업을 거쳐 만들어지는 시그니처에 의지하고 있을 뿐이고, 알려지지 않은 신종 위협에 대처하기 위한 보안 시스템의 개발 툴, 개발 절차, 배치 등과 같은 기술들은 너무 느리게 발전하고 있다.

본 고에서는 알려지지 않은 신종 사이버 공격으로 인한 피해를 최소화 하기 위한 대규모 프로젝트 두 가지를 소개하려고 한다. 이 프로젝트들은 신종 사이버 공격을 탐지하고 이를 차단하는데 사용하기 위한 시그니처를 생성하고, 해당 시그니처를 기존의 IDS/IPS 로 분배하는 역할을

수행하는 작업을 포함하고 있다. 이 프로젝트들은 유럽 연합에서 지원하고 있는 NoAH 프로젝트(Network of Affined Honeypots project)[4]와 한국의 정보통신부에서 지원하고 있는 ZASMIN 프로젝트(Zero-day Attack Signature Management INfrastructure project)[5] 이다.

II. NoAH 프로젝트

1. 서론

NoAH 프로젝트는 허니팟(honeypot) 기술에 기반하여 보안 모니터링을 위한 인프라의 개발을 위해 필요한 기술적인 작업들을 수행하고 디자인하는데 그 목적이 있다. 허니팟 그 자체로는 공격 차단을 위해 직접적으로 생성하는 것들이 없지만 대신에 망 자체를 의도적으로 취약하게 구성하여 유인된 공격들을 분석하기 위한 좋은 자료들을 제공한다. HoAH 는 초기 경보 시스템으로서 지리적으로 분포된 허니팟들을 사용하고, 공격 경보와 공격 차단 시그니처를 생성하는데 허니팟들에서 수집된 정보를 이용하게 된다.

NoAH 가 지향하는 것은 사이버 공격 발생시 NREN(National Research Network organizations)과 ISPs(Internet Service Providers)의 피해를 최소화 하고, 정보 보안 관련 조직들이 해당 위협에 더욱 능동적으로 대처하도록 하며, 연구자들에게 탐지 기술 향상을 위한 좋은 자료를 제공하는 것이다. NoAH 는 학계, 연구소, 산업체 등의 8 개의 파트너들이 참여하고 있으며, 유럽 연합의 연구 인프라 프로그램 (The Research Infrastructures Programme of the European Union)에서 지원하고 있다. 본 프로젝트는 2005 년 4 월에 시작하여 2008 년 3 월에 끝나는 3 년간의 프로젝트이다.

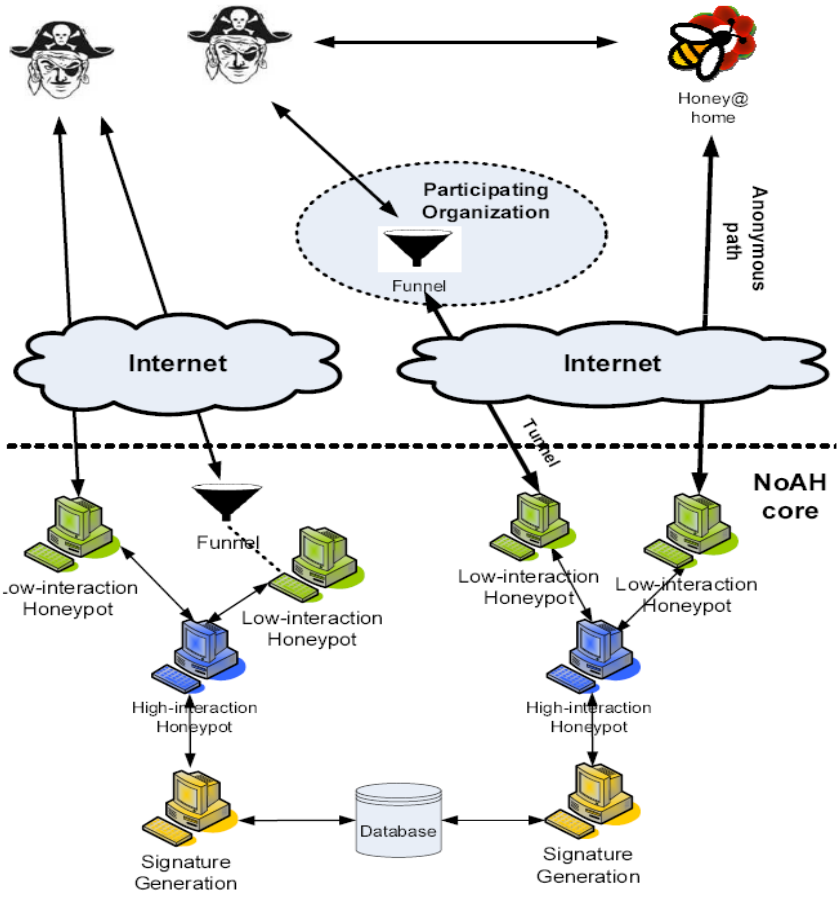
2. 운영환경

허니팟은 사이버 공격을 유도하기 위해 특별히 설계된 호스트들이다. 이 호스트들은 현재 사용되지 않는 IP 대역들을 이용하기 때문에, 허니팟으로 유입되는 모든 트래픽들은 대부분 악의적인 것들이다.

NoAH 는 두 가지 형태의 허니팟을 포함하고 있다. 하나는 로우-인터랙션(LI, Low-Interaction) 허니팟으로 실제 애플리케이션을 흉내내는 것처럼 서비스들을 에뮬레이션한다. 단

지 에뮬레이션 혹은 시뮬레이션만을 수행하기 때문에, 공격에 감염되어도 완전히 안전하다.

그러나 대부분의 경우에, 에뮬레이션 만으로는 알려지지 않은 취약점을 대상으로 하는 새로운 공격을 탐지하는 것이 어렵다. 하이-인터랙션(HI, Hi-Interaction) 허니팟은 이런 단점을 극복하기 위해 에뮬레이션을 하는 것이 아니라 실제 애플리케이션을 동작시키게 된다. NoAH 는 사용되지 않는 IP 주소들을 액세스 하거나 악성 트래픽과 상호 작용하는 허니팟으로부터 관련 자료들을 얻게 된다.



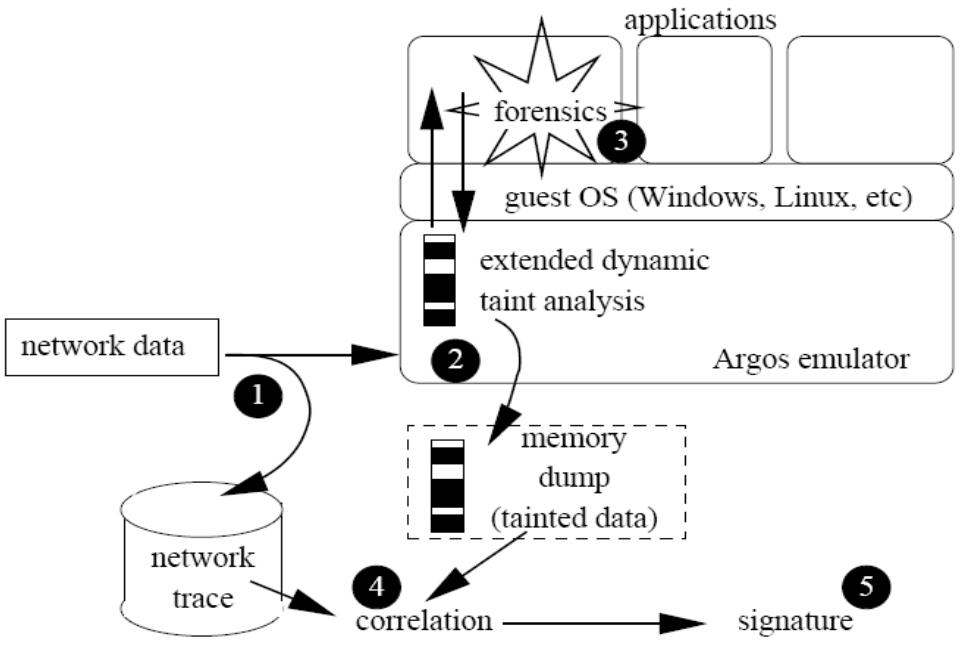
(그림 4) NoAH 프로젝트의 운영 환경

NoAH Core 는 허니팟들의 위치와는 별개로, zero-day 공격들의 자동화된 시그니처를 생성하기 위한 서비스들을 말한다. NoAH Core 에서 LI 는 트래픽 필터의 역할을 수행하며, 포트 스

캐닝과 같은 현상들을 효과적으로 탐지하게 된다. LI 에 의해 처리될 수 없는 트래픽들은 HI 로 넘어가게 되며, HI 의 감염으로 인한 피해를 막기 위해 관련 서비스들은 VMware, Xen 혹은 NoAH 프로젝트에서 제작된 Argos[6]와 같은 버추얼 머신(virtual machine) 상에서 동작하게 된다.

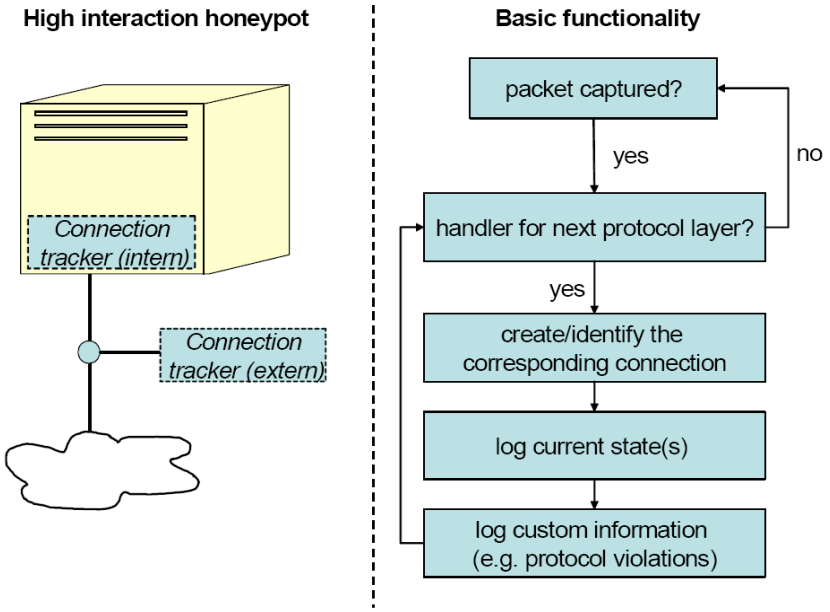
NoAH 가 처리하는 IP 주소 공간은 확장이 용이하며, 플러그인 모듈을 통해 캠퍼스 망, 기업 망 등의 사용되지 않는 IP 로 유입되는 트래픽들을 터널링(tunneling)을 통해 수집할 수도 있다. 또한 이와 같은 방식으로 사용되지 않는 IP 를 NoAH 와 공유할 수 있는 일반 홈 유저나 작은 기업들에도 적용하기 용이하다. 결국 NoAH 는 허니팟들의 유연성을 위해 다양한 네트워크와 호스트들과 유기적인 관계를 맺을 수 있다.

3. 시스템 구조



(그림 4) Argos 의 의심 트래픽 통제 환경

시그니처를 생성하는 NoAH Core 는 HI 허니팟에 Argos 라는 의심 트래픽 통제 환경으로 구축되어 있다. (1) 허니팟으로 유도된 네트워크 데이터가 Argos 에 도착되면, 해당 정보가 로깅되고 Argos 에뮬레이터로 보내진다. (2) 에뮬레이터는 입력된 트래픽을 tagging 하고, (3) guest OS 에서 해당 트래픽을 프로그램의 실제 입력으로 사용한 결과를 포렌직(forensic)한다. (4) 보안 정책을 위반하는 동작이 발생되면 해당 트래픽과 관련된 정보를 모두 dump 하여, (5) 시그니처를 생성하는 곳(SGC, Signature Generator Component)으로 전송한다.



(그림 5) 상태 추적기 동작 흐름

시그니처 생성을 담당하는 SGC(Signature Generator Component)는 각종 트래픽의 상태를 기록하는 상태 추적기(protocol tracker)와 Argos 로부터 이용 가능한 정보를 수집하여 시그니처를 생성하게 된다. Argos 에 의해 경고가 발생한 트래픽의 바이트 정보들은 각종 탐지 메커니즘에 의해 세부적으로 분석이 되고, 이 결과를 바이트 길이 분포와 바이트 빈도 분포와 종합하여 결과적으로 특정 패턴 형태를 가진 바이트들은 패턴 기반 시그니처로 제작할 수 있다. 이 때 탐지 메커니즘으로 이용할 수 있는 방법들은 기존의 방법들을 포함하여 다양하게 이용될 수 있다. 이렇게 최종적으로 생성된 시그니처들은 기존의 IDS/IPS 로 전송되어, 공격 탐지 및 차단에

이용되어진다.

III. ZASMIN 프로젝트

1. 서론

ZASMIN(Zero-day Attack Signature Management INfrastructure)은 네트워크 단에서 zero-day 공격이나 알려지지 않은 공격을 실시간으로 탐지하고 해당 공격을 차단하기 위해 사용되는 시그니처를 생성하고 관리하는 프로젝트이다.

(그림 6) ZASMIN 보안 카드와 시스템 실 사진

ZASMIN 은 개발 초기부터 상용화를 고려하여 설계가 되었으며, HW 기반 이상 트래픽 탐지 및 시그니처 추출 기술을 적용하여 고속 네트워크에서 실시간 적용이 가능하며, 생성된 시그니처 검증을 위한 공격 연관성 기능을 제공하여 해당 시그니처의 신뢰도를 향상시켰으며, 그 시그니처를 기존의 IDS/IPS 로 실시간으로 적용할 수 있어 공격 차단의 효율성이 뛰어나다. 이를 통해, 신종 공격에 대해서도 기존 보안 장비들의 재 사용성이 증가되며, 비 정상 행위 탐지의 높은

오탐율과 탐지 후 불 명확한 대응 기능을 보완할 수 있으며, 자동 시그니처 생성 및 이에 대한 정보 제공으로 CERT 팀의 업무 지원을 도울 수가 있다.

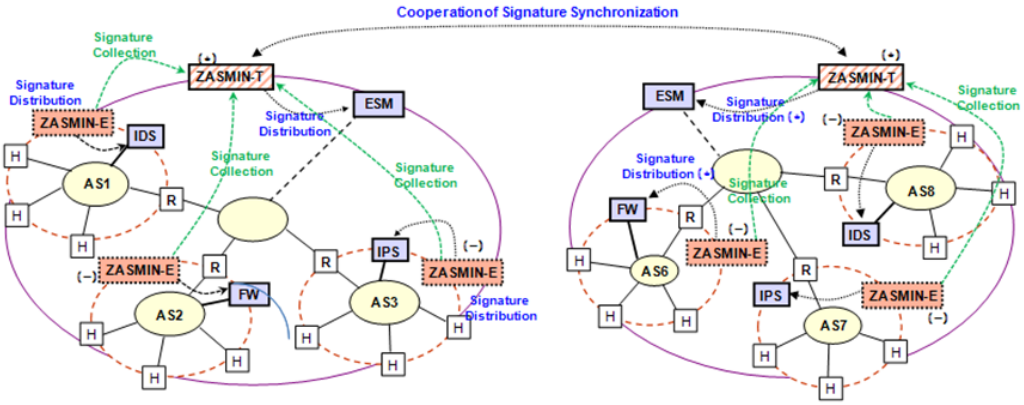
ZASMIN 프로젝트는 국내 대표적인 보안 업체들이 파트너로 참여하고 있으며, 정보통신부에서 지원을 하고 있다. 본 프로젝트는 2006 년 3 월부터 2009 년 2 월까지 3 년간 진행되고 있다.

(그림 7) ZASMIN 운영을 위한 GUI

2. 운영환경

ZASMIN 은 ZASMIN-T(Top level)와 ZASMIN-E(Endpoint)가 있다. ZASMIN-E 는 하나의 AS 레벨에서 발생하는 공격을 탐지하고 이에 대한 시그니처를 생성한다. 이 시그니처는 ZASMIN-T 로 전송이 되며, ZASMIN-T 는 다른 ZASMIN-E 로부터도 생성된 시그니처를 전송받아, 생성된 시그니처들 간의 연관성 분석을 수행한다. 그 후, 최종적으로 분배하기로 판단된 시그니처들이 ESM 이나 다른 ZASMIN-E 로 전송된 후 해당 AS 의 IDS 나 IPS 로 분배가 되고, 해당 보안 시스템들은 이 시그니처를 사용하여 현재 공격을 탐지하거나 차단하게 된다.

이와 같은 과정들은 수 분내로 실시간으로 이루어지기 때문에, 하나의 AS 에서 공격이 발생한다면 이미 그 시그니처들은 공격이 퍼져나가기 전에 다른 AS 들에 적용이 되어 공격을 차단하는 역할을 수행하게 된다. ZASMIN-T 에서 생성된 시그니처들 간의 연관성 분석을 하는 이유는 최종 시그니처의 신뢰도를 더욱 높이기 위한 작업이며, 유사 시그니처들을 제거하는 작업도 병행하게 된다.



(그림 8) ZASMIN 프로젝트의 운영환경

3. 시스템 구조

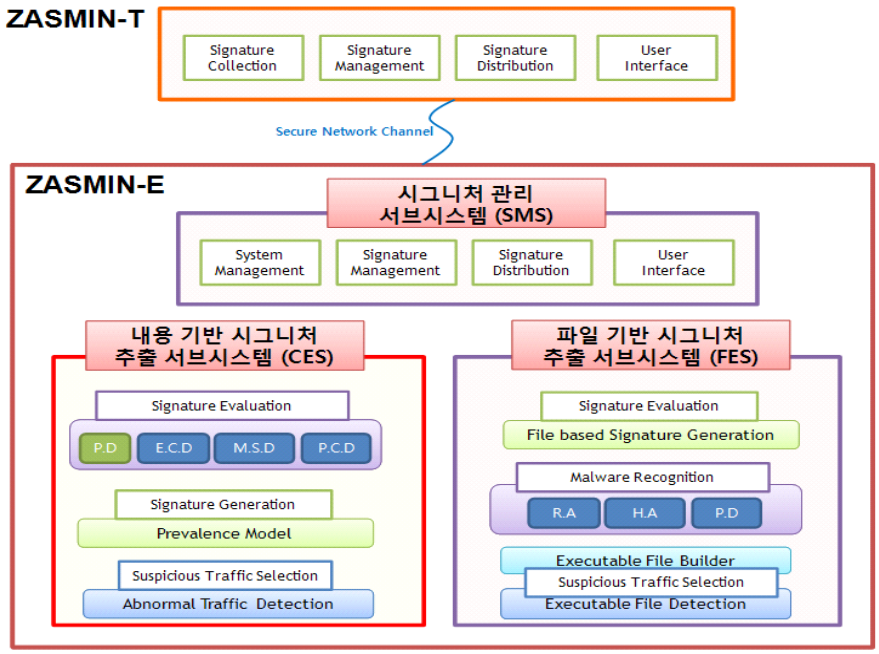
ZASMIN-E 는 하나의 AS 레벨에서 탐지활동을 수행하며 크게 CES, FES, SMS 세 가지 기능으로 구성되어 있다.

CES(Content-based signature Extraction sub-System, 내용 기반 시그니처 추출 서브 시스템)는 취약성을 가진 호스트들로 빠르게 퍼져 나가는 익스플로잇 코드(exploit code)나 웜 파일(worm file)을 탐지하여 이를 차단하기 위한 시그니처를 생성하는 역할을 한다.

ZASMIN-E 는 기가급 트래픽을 실시간으로 처리하기 위한 보안 카드가 장착되어 있으며, 이 보안 카드에서 주기적으로 주소 확산 정도(address dispersion), 세션 성공율(session success rate) 등이 측정되어 이상 탐지 분석 기능 (Abnormal Traffic Detection)으로 보내진다. 이상 탐지 분석 기능은 몇 주기 동안의 측정 정보를 분석하여 공격이 확산된다고 의심되는 3-tuple (source IP, destination Port, Protocol)을 선정하고, 패킷 캡춰를 위해 이를 보안 카드에 재 적용한다. 3-tuple 로 캡춰된 패킷들 속에 반복된 페이로드 패턴이 들어있는지가(Prevalence

Model) 분석되며, 이 반복된 페이로드 패턴으로부터 시그니처를 생성하게 된다.

실제 네트워크 환경에서는 여러 가지 이유로 공격이 아니지만 위와 같은 이상 트래픽 현상이 자주 일어나기도 한다. 따라서, 생성된 시그니처가 공격이 포함된 트래픽으로부터 생성되었는지에 대한 검증을 할 필요가 있다. 이와 같은 역할을 수행하는 것이 시그니처 평가 기능(Signature Evaluation)이며, 여기에는 실행 코드가 포함되어 있는지의 여부, NOP 이나 반복된 리턴 주소 같은 악성 코드의 포함 여부, 폴리몰픽 코드의 포함 여부, "/bin/sh" 같은 악성 스트링이 포함되어 있는지의 여부를 판단하여, 생성된 시그니처의 신뢰도를 판단하게 되고 신뢰도가 낮을 경우는 최종 시그니처로 활용하지 않게 된다.



(그림 9) ZASMIN 시스템 구조

FES(File-based signature Extraction sub-System, 파일 기반 시그니처 추출 서브 시스템)는 익스플로잇 코드에 의해 정복된 호스트로 전송되는 악성 파일(웜이나 바이러스 같은 실행 파일) 혹은 사용자가 오프라인으로 가지고 와서 AS 내부에서 돌아다니는 악성 파일 등을 탐지하여 이를 차단하기 위한 시그니처를 생성하는 역할을 한다.

ZASMIN-E 는 기가급 트래픽에서 실행 파일 헤더(PE 헤더, ELF 헤더 등)를 탐지하는 보안

카드가 장착되어 있으며, 이 보안 카드에서 실행 파일 헤더가 탐지되면 해당 세션의 모든 패킷들이 실행 파일 탐지 및 재조합 기능(Executable File Detection and Rebuiler)으로 보내진다. 해당 기능에서는 실행 파일의 여부와 재조합 가능성 여부를 판단을 하게 된다. 이렇게 재 조합된 실행 파일은 악성 파일 유무를 판단하는 기능(Malware Recognition)에서, 파일 packing 여부, 파일 헤더 이상 유무 등을 판단하여 최종적으로 악성 파일 여부가 결정된다.

IV. 결 론

알려지지 않은 신종 사이버 공격은 기존의 보안 시스템들로서는 탐지 및 대응 속도에 한계가 있다. 따라서, 전 세계적으로 이에 대한 연구가 활발히 진행되고 있지만, 높은 오탐율 등과 같은 여러 이유로 인해 실제 망에 적용되고 있는 사례는 드물다. 오탐율을 낮추고 대응 속도를 높이기 위해 신종 사이버 공격에 대비한 인프라 구축에 관한 프로젝트들이 다각도로 진행되고 있으며, 본 고에서는 유럽 연합의 NoAH 프로젝트와 한국의 ZASMIN 프로젝트에 대해 소개하였다.

두 프로젝트의 큰 차이는 시그니처를 생성하는 위치의 입장에서, NoAH 의 경우는 호스트 레벨이며 ZASMIN 의 경우는 네트워크 레벨이라는 점이다. 또한, NoAH 의 경우는 연구 중심적인 면이 강하며, ZASMIN 의 경우는 실 사용을 목적으로 설계되어 내년 초쯤 상용화가 예상되고 있다. 결론적으로 두 프로젝트는 각각의 장단점을 가지고 있을 것이며, 두 프로젝트의 결과들을 취합하여 앞으로 더 좋은 시스템 개발에 좋은 자료가 될 수 있으리라 생각한다.

<참 고 문 헌>

[1] CAIDA, www.caida.org.

[2] Lipson H. F, “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues,” Technical report, CERT Coordination Center, November 2002.

[3] E. Markatos and K. Anagnostakis, “NoAH: A European Network of Affined Honeypots for Cyber-Attack Tracking and Alerting”, The Parliament Magazine, Issue 262, 3 Mar 2008.

[4] NoAH project, www.fp6-noah.org.

[5] ZASMIN project, www.etri.re.kr.

[6] G. Portokalidis, A. Slowinska & H. Bos, “Argos: an Emulator for Fingerprinting Zero-Day Attacks”, Proceedings of ACM SIGOPS Eurosys 2006, April 2006.