악성코드 대응 MPSM기반 실시간통합분석체계의 설계 및 구현

윤종문*

요 약

고도화되고 지능화가 예상되는 사이버 침해대응에 대해 효율적으로 대응키 위해서는 악성코드의 공격에 대해 기존 방어적 대응형태에서 공격적 전환개념이 요구되기에 이러한 환경을 근간으로 연구한 결과 기존의 OS, APPLICATION SYSTEM 등의 각 영역별 SINGLE-MODE 체계의 구조대비 Real-time에 의한 공통 전수 취약점 탐지 분석 개념으로 다단계기반의 탐지 및 분석개념(MPSM)을 연구하였다. 동시에 필요시 해당 정보자산과 직접적인 단독접속형태의 취약점 탐지 및 분석을 위해 API 기반의 전용하드웨어 플랫폼형태의 방안이 요구되어 짐과 동시에 이를 위해서는 H/W 및 S/W의 분리된 현재와 같은 2중화된 형태가 아닌 일체형의 H/W 타입의 플랫폼구조 기반 형태로 설계됨과 동시에 병행되어 빅데이타 분석에 의한 정보보안의 포렌직 측면을 고려할 시 항시 모니터링 되고 관리할 수 있는 구조로 연동 설계 등에 대해 제안하였다.

Design and Implementation of a Real-time Integrated Analysis Framework based on Multiprocessor Search Modules against Malicious Codes

Yoon Jong Moon*

ABSTRACT

This dissertation introduce how to react against the cybercrime and analysis of malware detection. Also this dissertation emphasize the importance about efficient control of correspond process for the information security. Cybercrime and cyber breach are becoming increasingly intelligent and sophisticated. To correspond those crimes, the strategy of defense need change soft kill to hard kill. So this dissertation includes the study of weak point about OS, Application system. Also this dissertation suggest that API structure for handling and analyzing big data forensic.

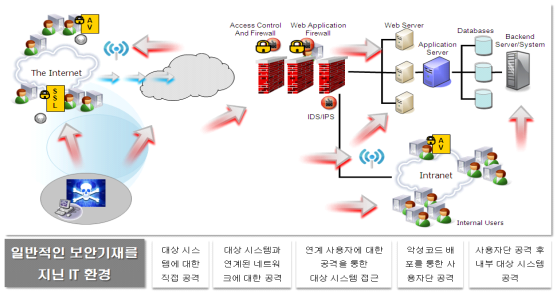
Key words: Multiprocessor Search Modules Esm Siem Sand-Box

접수일(2015년 2월 09일), 게재확정일(2015년 2월 24일)

* 경기대학교 산업보안학과

1. 서 론

정보보안은 관련 솔류션과 소프트웨어의 구비만으로 끝나는 것이 아니라 일련의 프로세스로서 구축된 보안장비와 해당시스템의 효율적인 운영을 통해 보안사고를 사전에 예방하고 대응하는 형태로 설계되어져야 한다. 특히 악성코드에 의한 보안위협은 이기종의 상황에서의 다양한 형태로 꾸준히 발생해 왔으며 방화벽 - 침입탐지 - 웹 방화벽 - 사용자PC 등의 정보 보안 구현은 더 이상 사이버 침해대응 위협에 대한 대응방법론의 측면에서 더욱더 관심있게 연구되어야 할 사안중의 하나인 것이다. 실질적으로 정부공공기관 및 사이버 대응 센터 등의 정보보안의 실무자들의 대부분이 악성코드 공격에 대해 좀더 향상된 방법으로 악성코드 탐지에 대한 여하한 적극적인 방안이 요구되는 것이다.



(그림 1) 일반적인 보안기재를 지닌 IT 환경

최근의 사이버공격은 이러한 기존의 방식과는 달리

1) 제로데이공격이나 루트킷(root-kit) 등의 매우 지능적인 보안위협을 이용 공격대상으로 정한 목표에 침투 후 중요한 정보를 수집하는 형태로 공격되는 양상이며

2) 공격대상의 방어체계에 탐지되지 않도록 은밀하고 끈기있게 오랜 기간에 걸쳐 공격을 진행하는 패턴의 형태를 보이며

3) 해킹능력과시나 계좌정보유출 등의 단순한 목적이 아닌 군사, 정치, 경제와 같은 고급정보를 수집하고 SCADA/ICS 등의 폐쇄망 환경에서의 구현된 국가 기간 시설을 파괴하는 등의 파급력이 큰 목적을 가지고 수행된다.

4) 또한 악성코드 자체에 대한 탐지를 우회하는 기법을 은닉화하므로서 업무영역은 물론 대국민서비스 인프라에 지대한 영향을 주는 것으로 연구되었다 .

<표 1> 정보 보호 관리체계구축 및 활용
보호항목수준

운영보안	매체보안
	악성코드 관리
	로그 관리 및 모니터링

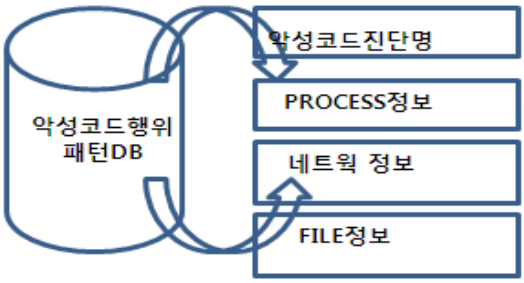
이에 기존 악성코드의 공격기술 동향분석과 이를 기반으로 한 정보시스템상의 현 대응방법에 대한 문제점 즉 정량화 및 정형화 형태의 프로세스화되는 현 취약점점검 방법과 기존 단순한 패턴 및 소프트웨어 기반의 취약점탐지 플랫폼 형태를 벗어난 Un-known 및 제로데이 공격 등의 장차 지능화되고 고도화되는 사이버침해공격에 대한 대응방안으로 전용 시스템 기반의 MPSM (Multi processor Searching Module)에 의한 취약점점검분석 ENGINE 기반으로 실시간 취약점탐지에 대해 각종 기산출 및 연구된 이론과 상용화된 테스트-TOOL을 활용 MPSM에 대한 타당성에 대한 고찰 및 이를 기반으로 API에 의한 ESM/SIEM 연동 구조 설계 연구와 예상되어지고 관심가져야 할 사이버공격대상 인프라인 사물인터넷(Iot) 및 폐쇄망구조의 산업제어망 (SCADA/ICS)등에 대한 효율적인 악성코드 대응방안에 대해 향후 연구해야할 주요 부분으로 제시하는 형태로 결론을 맺었다

2. 이론적배경

2.1 악성코드 취약점탐지분석형태

악성코드를 탐지하기 위한 기법은 해당 특정 프로그램의 악성여부를 판단하기 위해 그 프로그램의 정상적인 동작여부를 판단하는 명세기반탐지방법으로 이는 프로그램수행에 있어 유효한 동작에 대한 명세나 조건을 이용하는 것으로 그중 시그니쳐 기반 탐지방법은 특정프로그램 수행할 경우 나타나는 특징을 이용하

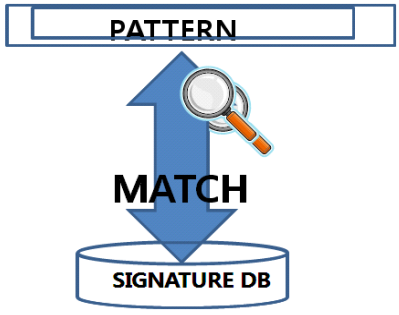
여 탐지하는 방법으로 이미 알려지거나 분석이 완료된 악성코드를 탐지하는 방법과 행위 기반 탐지 방법 및 유사도 분석을 탐지하는 방법과 같이 아직 un-known 및 기존악성코드의 변종을 탐지하는 방법으로 분류되며 일반적인 악성코드탐지방법은 하기의 구조 개념이다.



(그림 2) 악성코드 탐지패턴 BASE 정보구조

2.1.1 시그니쳐 탐지기법

시그니쳐 기반 탐지기법은 대부분의 안티바이러스 s/w에서 악성코드를 탐지하기 위해 사용하는 방법으로 하기 그림과 같이 악성코드 분석을 통해 추출한 특정문자열 signature를 data- base화하여 악성코드 검사대상이 되는 파일 내에 해당 문자열의 존재 유무를 판단함으로써 악성코드를 탐지한다. 해당탐지기법은 악성코드의 특정부분이나 고유한 부분이 검사 대상이므로 오탐지(false-positive) 및 미탐(false- negative)을 최소화할 수 있고 검사 시 파일의 특징적인 부분만을 비교하기 때문에 빠른 검사가 가능하다. 그러나 이미 분석이 이루어진 후 생성된 signature 가 존재하는 악성코드에 대해서만 탐지가 가능한 구조이므로 악성코드를 변형하여 생성한 변종이나 새로운 형태의 신규 악성코드는 탐지하기가 어려운 형태이며 최근에는 악성코드의 수와 종류가 급격히 증가하고 있기 때문에 수많은 악성코드들을 모두 수집하여 SIGNATURE를 생성하기가 쉽지 않을 뿐만 아니라 패킹기법이 적용된 악성코드에 대해서는 탐지가 거의 불가능하다는 단점이 있다.



(그림 3) Signature 기반 탐지기법 개념도

이러한 DB화된 Pattern-Data외에 발생되는 악성코드 이벤트에 대한 대응방안으로 우선적으로 탐지 및 분석을 Real-Time 및 상호연관분석 있는 구조로 설계가 요구되어진다.

즉 단순한 Pattern에 대한 즉각적인 대응은 물론 DB외에 악성코드에 대한 해당 이벤트 등에 대한 상황을 연계하여 ESM/SIEM과 연동 분석의 구조로 구현될시 악성코드공격에 대한 대응 수준을 제고할 수 있는 것으로 연구되어졌다.

2.1.2 해쉬함수 이용기법

MD5 해쉬 함수를 이용해서 악성코드에서 CRC (Cyclic Redundancy Check: 순환중복검사)대신에 안전한길이의 MD5를 추출하여 패턴DB로 활용하는 기법이다. 패턴에 적용하기 쉽고 CRC 탐지기법보다 오진율 발생이 거의 없으나 1Byte만 바뀌어도 탐지하지 못하는 단점이 있다.

2.1.3 소프트웨어 Tool에 의한 수동적 점검 형태

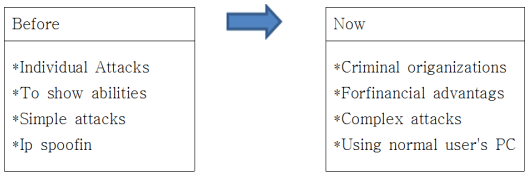
기존의 악성코드 취약점탐지 및 분석시스템은 해당 서버에 관련 tool 및 패턴을 설치하여 운용되는 구조이다. 즉, 공개된 WEB-TOOL 또는 해당 open-source나 자체적으로 개발된 취약점 형태로 해당 악성코드공격에 대한 취약점을 진단 및 분석하는 구조인 것이다. 이러한 형태의 특징은 최적화 및 신뢰성 등이 검증되지 않은 형태의 패턴 및 라이브러리로 구현되는 형태로 인해 해당 취약점이 발생되어 공격의 환경을 제공하게 되는 것이다.

특히 취약점 관리 분석에 대한 주체가 외부에 의뢰하는 컨설팅업체가 진단 및 분석을 하여 구현되어지는 구조이다.

또한 필요할 시 또는 점검상의 관련된 규정(Compliance)에 의해 수행되어지므로 인해 년 1회 분기 1회 등으로 수행범위 및 횟수가 한정적이므로 인해 악성코드 및 기타 사이버침해에 대해 지속적인 관리는 제한적이며 단순환 형태로 진행되는 구조인 것이다. 병행하여 이러한 취약점 tool은 수동화되고 제한적인 형태이므로 지속적인 관리에 애로사항이 있으므로 인해 계속적인 오탐과 미탐에 대한 관리가 실시간적으로 행위를 할 수 없는 사안이므로 적극적이고 능동적인 형태의 사이버 침해대응을 위해서는 In bound-Out bound의 내외부 악성코드탐지가 가능한 구조로 구현되어져야 할 것이다.

3. MPSM 연구 분석 설계 및 분석

인터넷환경의 발달로 인하여 갈수록 다양해지고 정교해지는 악성코드들을 탐지하기 위한 많은 연구들이 진행 중이지만 악성코드의 발전 속도에 적극적으로 대응하지 못하고 있는 상황인 것이다. 이러한 환경을 고려할 시 악성코드를 탐지대응하는 기법을 개발하기 위해서는 탐지하고자 하는 악성코드의 종류 및 특징에 대한 분석이 선행되어져야 한다.



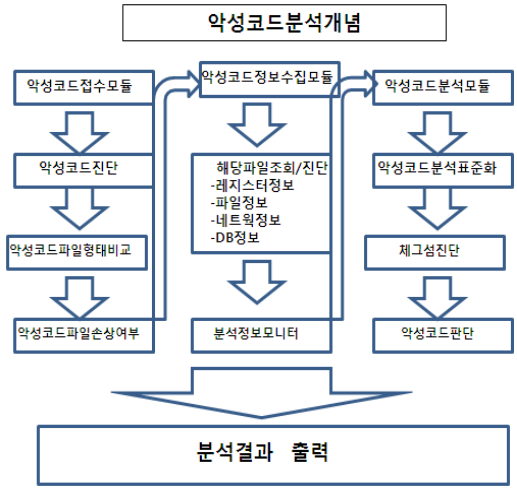
(그림 4) 인터넷 공격의 변화

이와 같이 다양한 연구에도 불구하고 변종 악성코드에 대한 정적 분석 방법은 계속해서 진화하는 코드 난독화 기술로 인해 악성코드가 실제로 수행하는 행위를 판별하는데 많은 어려움이 존재되는 구조이다. 동적 분석은 모니터링이 가능한 환경에서 악성코드를 실행하여 행위를 관찰하거나 분석하는 과정을 말한다. 동적 분석을 통해 파일, 레지스트리, 프로세스, 네트워크 등의 활동 정보를 얻을 수 있다. 따라서 실행 압축과 코드 난독화 기법 등에 상관없이 실제 악성코드가 수행하는 행위를 분석할 수 있다는 장점이 존재한다. 이에 <표 2>는 악성코드가 수행하기 위한 행위에 따라 분석에 이용 가능한 API들의 예를 나타낸 것이다.

<표 2> 악성행위 분석에 이용가능한 API의 예

Target	Apis
File	Create File() Copy File()
Registry	Reg Create Key Ex() Reg Open Key Ex()
Process	Create Process() Terminate Process()
Network	Send()/reLcv() Connect()

Windows PE 파일형태의 악성코드 샘플을 제출하면 동적 분석에 대한 상세분석을 제공하여 주는 형태로서. 제공되는 악성코드의 행위분석 내용으로는 파일 변화, 레지스터의 변화, 프로세스 변화, 네트워크 연결 등에 대해 기존악성코드공격에 대한 행위 등을 분석할 시 이에 대한 적극적인 대책으로 악성코드 분석 자체를 역으로 차단 탐지할 수 있는 다단계 SIGNATURE 기반의 플랫폼 형태의 분석방법론이 요구되는 것이다.



(그림 5) 악성코드 분석 개념

이러한 악성코드는 바이러스백신과 스팸메일차단시스템과 같은 보안장비에서 차단하지만 UN- Known 및 zero-day에 대한 악성 코드의 경우 탐지하기가 어렵다. 이를 위해 해킹메일에 감염된 시스템을 탐지하기 위해서는 네트워크 패킷을 이해하고 전산망환경에 맞는 최적의 규칙을 생성해야 하며 이를 위해서는 감염신호전송탐지패턴, 악성코드다운로드탐지패턴, 내부시스템정보유출탐지패턴, 자료 유출경유지 탐지 패턴 등이 요구되는 것이다. 이러한 일반정보유출 악성코드를 감염 및 공격하였을 경우 침입탐지시스템에서 감지한 결과 모두 동일한 특정 패턴에 의해 감지된 것으로 탐지가 가능했다.

<표 3> 일반적 정보유출 추출 패턴 탐지결과

구분		일반적 악성코드	해킹메일 악성코드
패턴기반	다운로드	탐지	탐지
	내부 자료유출	탐지	탐지

아래의 표는 해킹메일악성코드에서 추출한 패턴을 보안장비에 적용하여 일반적인 악성코드와 해킹메일 악성코드를 감염시켰을 경우 침입탐지시스템에서 감지한 결과이며, 특정패턴과 IP기반 패턴에 의해 감지된 것으로 일반적인 악성코드에서 신호전송과 자료유출경유지는 감지 못했다. 이는 두 가지 경우 네트워크 트래픽을 발생시키지 않아 탐지되지 않았다.

이러한 환경을 고려할 시 연구되어진 현황 등을 고려할 시 각 분석방법에 대해 향상된 오탐과 미탐에 대한 대응측면에서 좀더 고도화되고 지능화된 탐지체계가 요구되는 것이다.

<표 4> 추출 패턴 탐지결과

구분		일반적 악성코드	해킹메일 악성코드
패턴 기반	다운로드	탐지	탐지
	내부 자료유출	탐지	탐지
	신호전송	미 탐지 (신호 미발생)	탐지
IP 기반	자료유출 경유지	미 탐지 (신호 미발생)	탐지

3.1 MPSM 개념

3.1.1 MPSM의 설계 Process

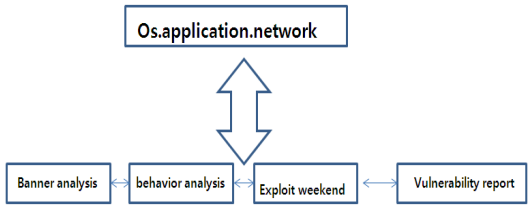
악성코드 공격에 대한 오탐과 미탐을 최대한 줄이면서 해당영역별 취약점 결과에 대한 상호연관성분석과 사용자의 점검 정책 등에 대해 일관성 및 연속성을 보장받을 수 있는 MULTI- MODE 개념의 탐지/분석 엔진이 절대적으로 요구되는 것이다. 이러한 MPSM의 개념

1) Multi-mode가 취약한 장치의 버전, 종류, 서비스 팩을 분석, 해당보안취약점을 결정하는 프로파일링을 구현한다.

2) 취약한 장치에 다른 종류의 유효한 데이터와 유효하지 않은 데이터를 보낸 후 반응을 검사하여 보안취약점의 영향을 받았는지를 검사함

3) 침투테스트 시나리오를 구성하여 스캔된 장치에 있는 세부적인 취약점분석

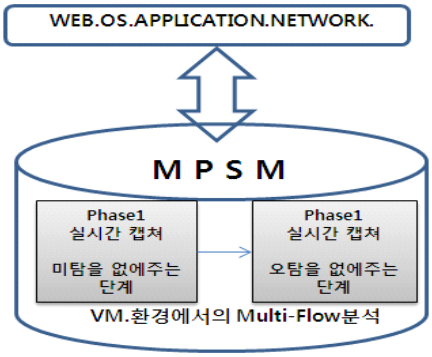
4) 실제의 취약점에 대하여 통합리포트제공의 구조로 실현되어지는 형태이다.



(그림 6) 다단계 취약점 탐지시스템 설계

3.1.2. MPSM의 아키텍처 설계 연구

MULTI PROCESSOR SEARCHING MODULE 은 악성코드의심파일에 대해 가상머신에서 실제 실행한 결과를 기반으로 분석하므로 정확한 분석과 정보반영이 가능하며 장기간에 걸쳐 시행되는 공격에 대해서도 효율적인 탐지와 차단이 가능한 구조인 것이다. 이에 대한 아키텍쳐는 하기의 형태로 개념되어 진다.



(그림 7) MPSM 개념

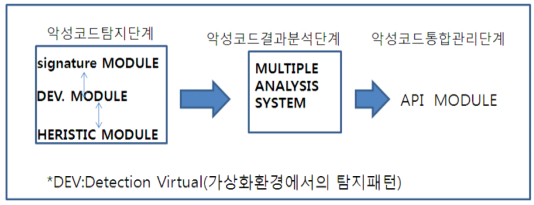
가상화 기반의 sand-box 기본구조로 실시간 분석에 대한 구조로 웹, 시스템, 네트워크 등의 악성코드 공격에 대해 Crawling방법론에 의한 전수 취약점분석을 수행하는 개념으로 설계되는 구조이다

즉 악성코드의 공격유형을 패턴화할 수 없지만 대체로 취약점탐색→유인→침투→수집 확산→정보유출 혹은 시스템파괴의 processor로 구현되는 공격형태를 고려할시 공격자는 목표시스템의 취약점을 탐지하여 주요한 정보를 수집과 동시에 또 다른 공격을 위해 시스템내부에 영역을 확산시킨다. 이러한 현상을 고려할시 우선적으로 악성코드에 대한 방어를 위해 최초 침입단계에서 악성코드에 감염 가능한 의심스러운 파일을 탐지 분석하는 기술인 샌드박스로 설계됨으로서 악성코드의 다양한 우회공격이 가능하고 인라인 구성이 어려워 제로 데이 공격을 방어하는데 한계에 대한 부분 등에 대해 의심파일을 미러링하여 가상화 환경에서 해당파일을 탐지 삭제 및 분석하는 방식으로 구현되어지는 샌드박스 형태로 설계되어져야 하는 것이다.

<표 5> MPSM과 기존 방법론과의 차이점

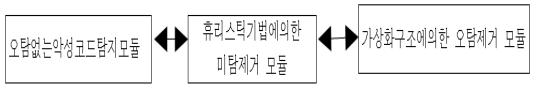
multi processor SEARCHING moduel	행위기반분석
전용하드웨어 플랫폼	appliance타입
multi-flow분석	개별(어플리케이션, 시스템, 네트워크 등) 단위분석
vm회피악성탐지가능	vm회피악성탐지불가
최적화된 성능 및 기능제공	서버에 탑재되어 운용되므로 성능 및 기능제한
exploit분석	분석불가

MPSM시스템구성도



(그림 8) MPSM 시스템 구성도

악성코드탐지단계에서의 기존의 악성코드를 진단하기 위해 악성코드를 debugging 해서 내부의 특정코드를 수집하고 이를 DB화하는 구조로 설계되어지는 HEURISTIC을 참고로 연구하였다. 이러한 DB패턴을 활용하여 변종 및 신종 악성코드에 대해서는 직접적인 대응방안이 제한적이므로 heuristic-module이 기존 탐지방법론에 비해 진보화된 MODULE이므로 이를 설계할 시 지금까지 발견된 악성코드에 기반하여 향후 악성코드를 미리 예측하여 발견할 수 있는 구조이다. 이러한 환경에 의해서만이 기존의 각각의 영역 또는 카테고리별(os.app.system) 제한적인 분석 대비 multi-flow가 가능하며 정보보안 환경을 회피한 형태의 악성코드 공격에 대한 대응이 가능한 것이다. 병행하여 이미 알려진 정의된 악성코드에 대한 탐지 및 식별은 물론 빠른 변종에 대한 대응(zero-day공격)과 오탐 및 미탐 등에 대한 행위기반 분석구조에 대한 새로운 형태의 대응방법이며 이러한 구조는 탐지단계 - 결과분석단계 - 통합관리단계의 PROCESS 구조로 설계되어짐과 동시에 특히 탐지 단계 및 결과분석단계는 전용 단일 플랫폼에 의해 구현되어지므로 실시간 및 분석을 수행할 수 있는 기반요건이 되는 것이다.



(그림 9) MPSM 수행구조

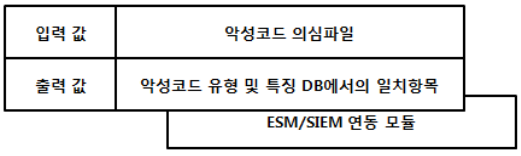
3.2 Real-Time에 의한 악성코드 탐지 구현

3.2.1. 실시간 취약점 분석 구현

악성코드에 대한 실질적인 탐지와 분석으로 효율적인 침해대응을 위해 우선적으로 실시간적 구현이 processor가 중요한 요소인 것이다. 이를 구현키 위해서는 web을 통한 contents를 access하는데 있어서 보다 향상된 기능 및 편의성이 요구되면서 기존의 방법에 대한 한계성으로 인해 java-applet, 자바 script, 그리고 activeX- contrL 등과 같은 다양한 실행코드 기술들이 발전과 동시에 각종 실행코드의 배포가 활발해지고 있다. 그러나 activeX-contrL 등의 실행코드들은 사용자가 직접 의도했던 행위 대신에 LOCAL 자원에의 불법적인 접근 및 시스템 파괴와 같은 악성행위를 수행할 수 있다.

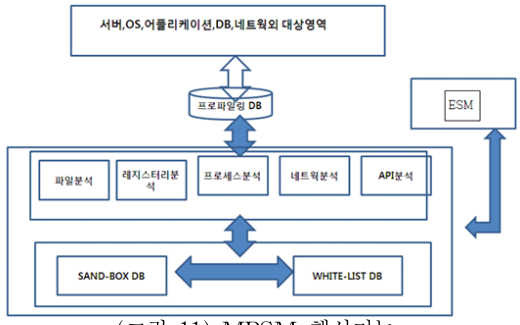
3.2.2. MPSM REAL-TIME분석 구현

본 연구에서는 각 영역별(OS, APPLICATION, DB 등)에 대해 별도의 각 카테고리에 대한 특정DB의 분석방법에서 탈피 해당 프로파일 DB에서 파일, 레지스트리, 프로세스 등에 대해 각각 코드 유사도 계산 등의 방법론을 통해 악성코드의 유형 및 코드에 대한 선행분석을 수행되는 기반 환경에서, 이를 자동화분석하여 각각의 악성행위 및 코드 특징 등을 도출한다.



(그림 10) 악성코드 의심파일 Report

이를 위한 선행 단계로써 수행된 특징 단계의 이벤트를 상호작용 단계를 거쳐 악성코드의 특징 DB가 마련된 후, mpsm의 프로파일링 분석 단계에서 악성코드로 의심되는 파일이 INPUT값으로 주어지면 특징 도출 프로세스가 해당 파일을 분석한다. 따라서 악성코드 특징 DB에 저장된 데이터와 특징 도출 프로세스에서 도출된 결과들은 프로세스에 의해 비교가 REAL-TIME으로 구현되어짐으로써 악성코드 의심파일에 대하여 분석 결과 및 악성코드의 유형을 리포팅하게 되는 구조인 것이다.



(그림 11) MPSM 핵심기능

3.2.2.1 시스템 구성

MPSM은 다양한 취약점 점검 도구를 원격에서 제어하고, 점검 결과를 수집하여 통합 분석할 수 있는 구조이다. 이러한 기능들은 MPSM을 구성하는 취약점 점검 도구 에이전트, 취약점 탐지 관리 및 통합매니저, 취약점 점검 제어 및 분석 센터에 의해 구현된다.

악성코드 침입탐지모듈에서는 프로세스별 전체 이벤트 위험도를 누적하고 이 누적된 위험도가 악성행위로 판정되기 위한 임계값을 초과하는지 판단하여 초과하는 경우에는 프로세스의 실행을 중지시키고 해당 프로세스에 대한 정보와 위험도가 부여된 2차 로그를 관리 서버에 전송한다. 이때 임계치 값은 사용자가 설정한 보안등급에 따라 달라질 수 있는데 본 설계에서의 보안등급은 "높음", "보통", "낮음"으로 구분하도록 함으로써 사용자 영역에서의 사용 편리성을 제공하여야 하는 구조이다

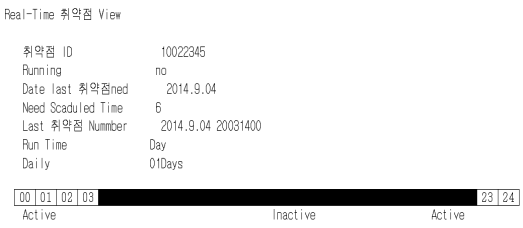
특히 네트워크 단절과 같은 상황에서도 에이전트는 자체 DB에 해당탐지 결과를 임시 저장하고 있다가 관리도구와의 통신이 재개되면 즉시 해당정보를 자동으로 관리서버에 전송하도록 함으로써 한번 탐지된 악성실행코드는 즉시 필터링하는 구조로 구현되어야 한다. 이러한 개념에 의거 관리서버, 스캔서버 그리고 일체형 등으로 구현 설치되어져야 한다.

스캔 대상 서버에 대해 목록 기술 및 스캔 실행기능과 스캔유형 사용자정의 등이 제공되어야하며 실시간 스캔을 하기 위해 해당 시간대에 대한 TIME-스케줄이 구현되어야함과 동시에 TIME- SCEDULE에 대한

취약점VIEW는 타계정과의 상관분석 등을 위해 해당 IP주소 해당자산에 대한 위험도표시 DNS 등에 대한 상세정보 등이 요구되어지므로 이에 대한 관련 설계는 하기와 같은 취약점-View형태로 제공되어야 한다.

LOCATION	VALUE	Operation System	DNS	NET BIOS	MAC
192,168,164	RAW	UNIX3.3	UN-KNOWN	UN-KNOWN	UN-KNOWN
192,168,184	HIGH	LINUX 2.3.3	ERT.COM	ADFER	00.6C.45.21
192,143,121	MEDIUM	WIN7	MOPAS.COM	WEFGM	02.39.45.00

(그림 12) 스캔 대상 서버 목록



(그림 13) Real-Time 취약점 View

location	Total	High	Medium	Low	Score	Trend	Report
Unix2.3.	4	4	-	-	4	RISK	Word Excell.Pdf
linux 5.6	2			2	2	-	Word Excell.Pdf

(그림 14) 해당기관 보안 취약점총계

Location	취약점	Vulnerability Name	Risk	IP	취약점 Date
Sever Farm Dmz 1	System server	Ftp Empty UserName &Password	High	134.359.324	2014.08.04

(그림 15) 자사별 해당 보안 취약점 View

상세정보일자:0000Y00M00
취약점형태:FTP EMPTY USERNAME AND PASSWORD
위험도:상
호스트명/IP주소:192.160.1.252
서비스프로토콜:FTP/TCP
서비스군:FTP서버
상태:취약점결과 상세설명 제공
위험정도:파일데메지 및 암호화키 변조
방안:PW재설정 및 암호화방식변경
CVE:CVE-1999-0452
CVSS 점수:4.9

(그림 16) 취약점 스캔 결과

각 해당별 View에 대한 취약점 결과에 대해 발생위치 및 내역, 일시, 위험내역, 해결방안 등에 대해 상기와 같은 형태로 Mpsm의 real- time에 의한 취약점에 대한 결과를 사이버 침해 대응 측면에서 단순한 해당 취약점 콘솔형태로 국한되어 운용되어지는 것이 아니라 타 정보 보안 및 자산등과의 상호관계를 고려한 종합적이며 통합적인 설계가 요구되므로서 즉각적인 대응을 할 수 있으므로 이를 위해 API 기반에 의한 ESM 또는 SIEM과의 연동 구현되므로서 MPSM 기반 하에 지능화되고 고도화된 취약점에 대한 대응을 할 수 있는 것이다. 즉, 자동스캔 대상서버에 대해 목록기술 및 스캔실행기능과 스캔유형 등의 사용자 정의 예약설정 등을 통해 요구하는 시간대에 스캔을 함으로써 정보보안의 연속성이 보장되어진다.

3.3 MPSM과 통합보안운영관제 연동방안 연구

3.3.1 MPSM과 ESM연동 필요성연구

ESM의 일반적 구조는 논리적인 3계층 또는 4계층으로 나눌 수 있다. 3계층구조는 보안시스템들과 다양한 장비에서 이벤트를 실시간으로 수집해오는 Agent-Part, 중앙에서 통합적으로 Agent 의 이벤트를 받아서 분석하여 그 결과를 DB에 저장하고 콘솔에 실시간으로 전송하는 Manager Part, 그리고 사용자가

보안정책을 설정하고 로그를 분석할 수 있는 Consol Part, 이렇게 3계층으로 구성된다.

(그림 17) ESM의 3계층 구조

이러한 관리체계는 보안장비의 이벤트 발생을 인지하고 분석하여 적절한 대응을 하는 절차로 진행된다. 여기서 중요한 것은 보안장비의 이벤트 발생을 인지하는 것이다. 이러한 이벤트 발생을 신속히 인지할수록 신속하게 대응하여 피해를 줄일 수 있기 때문이다. ESM은 보안장비의 이벤트를 통합적으로 모니터링하고 관리할 수 있다는 장점이 있지만 이벤트 발생을 인지해야 하는 것이다.

3.3.2. 악성코드 대응 관련 ESM/SIEM 연구

일반적으로 보안관제 업무는 악성코드의 대응을 위한 해당 이벤트 발생을 인지하고 분석하여 적절한 대응을 하는 절차로 진행된다. 여기서 중요한 것은 악성코드의 이벤트 발생을 인지하는 것이다. 이벤트 발생을 빨리 인지할수록 신속하게 대응하여 피해를 줄일 수 있기 때문이다. ESM은 보안장비에 대한 통합적으로 모니터링하고 관리할 수 있다는 장점이 있지만 그만큼 많은 보안 이벤트의 발생을 인지해야한다는 문제점이 있다. 하기의 통계표가 제안하는 의미는 이벤트 발생을 모니터에 표현해 주는 TOP-DOWN 방법과 발생횟수 누적방법도 많은 양의 이벤트를 화면에 UI로 제공되기 때문에 주의 깊게 모니터화 되지 않으면 중요한 악성코드 발생에 대해 즉각적으로 대응하기가 제한적인 형태인 것이다.

<표 6> ESM이 수집한 보안장비 이벤트/1DAY 발생통계

구분	이벤트명	발생건수
네트워크 침입탐지1	50	23,317
네트워크 침입탐지2	73	42,083
웹방화벽	45	22,098
네트워크 침입예방시스템	23	45,923
합계	191	133,421

이러한 현상을 근간으로 취약점 상관분석 및 취약점에 대한 상세관리 및 이벤트에 대한 통제 및 관제기능 구현이 미설정 되어 있는 현실인 것이다. 이에 대해 해당 관제기능과 MPSM에 대한 연동방안에 대해서는 우선적으로 해당API를 구현하여 PROCESS화 하는 것을 요구되는 것으로 이에 대한 보안관제 기능은 REAL-TIME 모니터링 및 침입 분석이 가능한구조가 되어야하며 각 시스템 또한 이기종 이벤트를 실시간으로 직관적인 방법으로 상호 연결 분석하고 이기종 IDS의 서로 다른 위험도 평가에 정형화된 기준을 제시한다. 이러한 이벤트들은 REAL- TIME 알림, SOUND, 이메일, SMS 등 다양한 방법으로 정보를 제공하며 위험 등급 관리에 의한 임계치 지정 및 경보 기능등을 활용해야 할 MODULE인 것이다

<표 7> 국내 통합보안관제 기능 비교표

구분	상세기능	00사	AA사	BB사
보안로그 이벤트 발생지원	SMS/EMAIL /모니터링화면	지원	지원	지원
네트워크 위험도	통합적 위험도	지원	지원	지원
	개별적 위험도	지원	일부지원	일부지원
	특정이벤트 대상	지원안함	지원안함	지원안함
취약점 상관분석 이벤트관리	이벤트생성	지원불가	지원불가	지원불가
	취약점발생 이벤트모니터			

이러한 ESM의 보안관제기능의 상관분석기능을 사용하여 관련 이벤트에 대한 미탐 및 오탐을 줄일 수 있는 인프라가 구현되어야 하는 것이다. 이를 위해서는 기존의 모니터링 되는 정보보안제품 외에 원래의 목적인 사이버 침해 대응에 대한 통합관리를 위해서는 현재 접목되어 운용되는 정보보안자산 외에 업무시스템 및 기타 시스템은 물론 실시간으로 취약점 이벤트를 관리Consol로 해당 분석된 취약점에 대해 동시에 관련된 인프라에서 대응할 수 있도록 필수적으로 구현되어야 함은 물론 이러한 알려진 해킹 패턴 외에 Un-Known, 제로데이등에 대한 적극적인 대책으로 통합보안관리(ESM)영역의 범주에 실시간 취약점 탐지 분석 매커니즘 분야가 설계되어짐으로서 향후 예상되는 사이버침해에 적극적으로 대응할 수 있는 구조가 마련되는 것이다.

3.3.3. MPSM과 통합보안운영관제(ESM/SIEM)과의 연동 방안

이러한 ESM은 방화벽, IDS. IPS. VPN 등 이기종 보안시스템을 중앙에서 통합 관리하는 단순한 범주를 벗어나 예상되는 향후의 침해대응 및 cyber-terror에 대응키 위해 기 논술된 악성코드 공격에 대해 즉각적으로 관제 및 관리할 수 있는 구조로 구현되어야 함으로 이에 대한 방법론의 MPSM의 플랫폼을 WEB기반으로 구현하는 환경을 구현해야 함이 요구되는 것이다. 이러한 연동방안을 위해 구현되는 설계 구현개념은

1. 상관 분석에 의한 이벤트의 인덱싱 (INDEXING)

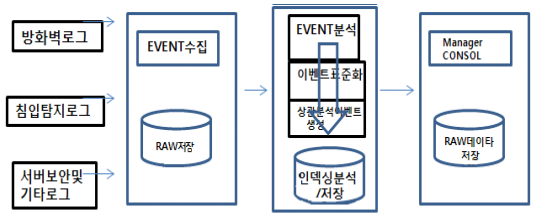
ESM과와의 MPSM과의 연동방안을 제시하기 위한 개선방안을 API에 의한 통합 구현개념형태로 설계하고자 하는 것으로 기존 ESM의 보안관제중 기능의 문제점 중 기 연구된 바와 같이 인지해야 할 EVENT가 너무 많고 이벤트를 인지하는 방법에 개선해야 할 요소가 있음을 기 논고한 바 있다. 이 부분을 해결하기 위해서 필요한 것은 우선 인지해야 할 요소를 최소화하고 운용자가 이벤트를 인지할 수 있게 하는 구조로 유형별로 최대한 색인화하는 즉 INDEXING화하는 것이 우선 전제조건이다.

1-1 인덱싱 이벤트 CRAWLING

먼저 인지해야할 이벤트를 줄이기 위해서 해당 통합보안관제의 인덱싱 기능을 설계해야 한다.

인덱싱은 많은 이벤트에 대해 빠른 SEARCH를 위해 상관 및 유사한 이벤트를 최대한 그룹핑하여 새로운 이벤트명으로 생성하는 구조이다.

이런 논리로 많은 이벤트를 최소화와 SEARCH ANALYSIS화 할 수 있는 것이다.

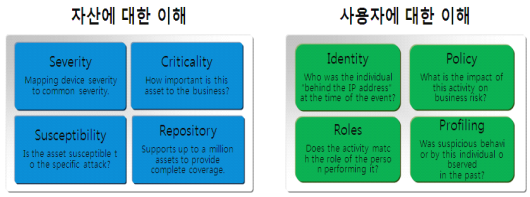


(그림 18) INDEXING-PROCESSOR

3.3.4. MPSM-ESM/SIEM과의 상관관계 설계

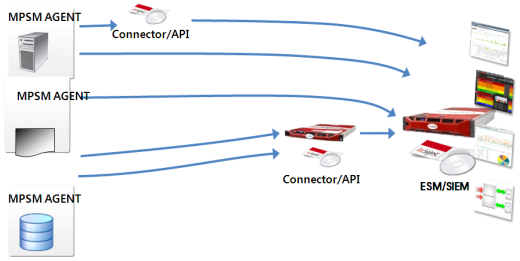
지능화되고 고도화되어가는 악성코드에 대한 대응을 위해서는 우선적으로 현재의 통합보안관리(Esm/Siem)은 각종 데이타에 대한 무손실처리로 악성코드에 대한 오탐 및 미탐에 대한 대응방안을 우선적으로 설계해야 되며 보안 외 이기종의 다양한 자산(시스템, 네트웍외)에 대한 통합관리를 하기 위해서는 기존 구축된 관제모니터링 툴과의 호환 및 연동구축과 실시간 즉석/상관분석으로 해당 악성코드에 대한 장애원인 분석과 이에 대한 리포팅 등이 관심있는 기능으로 발전시켜 가야 하는 것이다.

<표 8> 상관분석의 요구사안

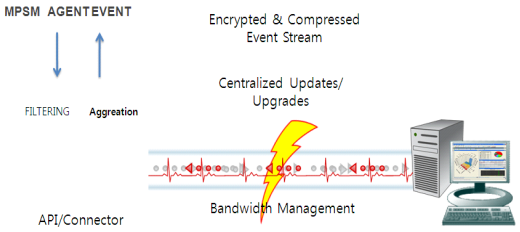


즉 이러한 상관관계 분석으로 인해 실제 악성코드의 위험과 보안경고의 문제점인 false- positive(오탐 및 미탐)에 대한 실질질인 대응으로 실제적인 위협과

위험에 대한 공격적 방어를 구현 할 수 있는 FOCUSING이 가능한 구조인 것으로 이를 위한 MPSM과와의 연동 아키텍처는 MPSM에 수집되어지고 우선적으로 분석되어진 이벤트는 CONNECTOR 또는 API 모듈에 의해 SIEM / ESM의 통합관리 메니저로 해당 데이타를 송수신하게 되는 형태로 설계되므로서 실시간 상관분석으로 악성코드 취약점에 대한 이벤트의 원인을 분석할 수 있는 구조가 되는 것이다.

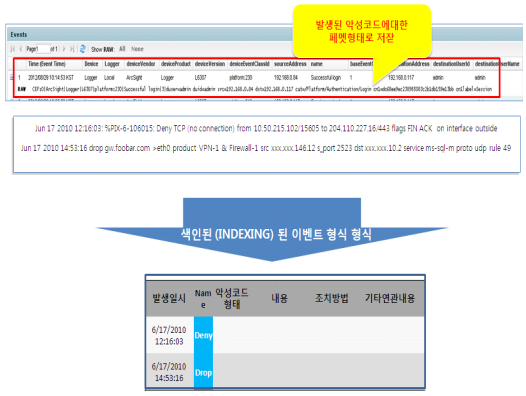


(그림 19) MPSM의 수행 구조



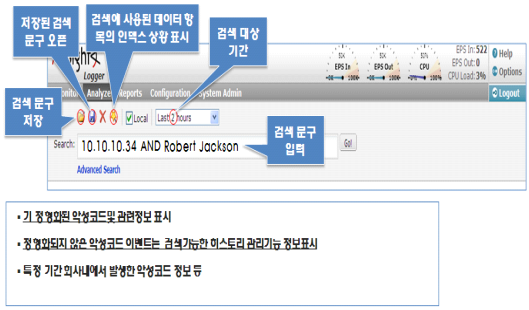
(그림 20) MPSM -AGNET /SVR와의 데이터 무손실 구조

이러한 프로세스로 인해 수집된 악성코드관련 이벤트를 SIEM/ESM에 구현 및 연동키 위해서는 운용자가 용이하게 접근할 수 있는 템플릿화 구조로 구현되므로서 실시간적을 상관분석을 수행할 수 있는 요구조건을 구현한다고 판단된다.



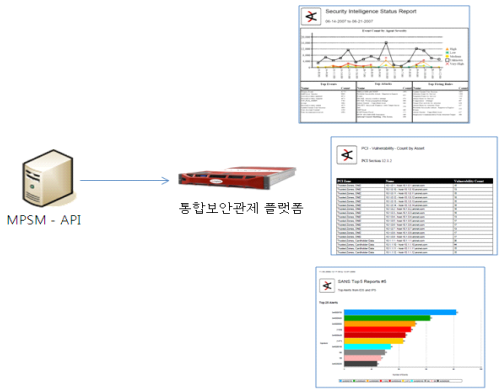
(그림 21) 통합보안관제 악성코드 인덱싱구현

MPSM에 의해 구현된 악성코드이벤트는 운용자 및 관련관리자 등이 계속적인 운용을 위해 수집되어 상관분석된 악성코드의 유형에 대해 향후 즉각적인 침해대응을 위해 해당 악성코드 이벤트에 대한 용이한 검색 및 인터페이스환경구조를 위해 검색엔진의 형태로 설계되어야 하는바 이에 대한 개념 설계는 아래와 같은 구조로 설계될 시 좀더 고도화된 사이버 침해대응 분석메카니즘이 형성된다고 판단되어진다.



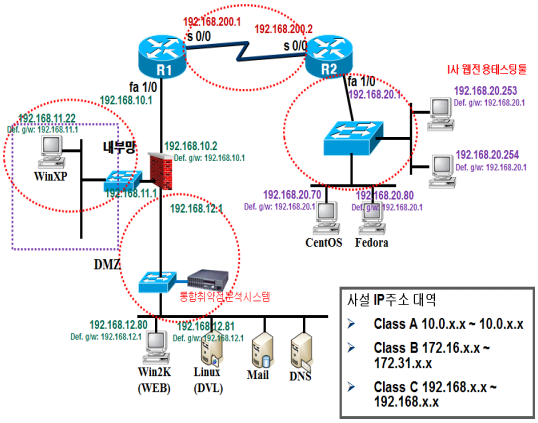
(그림 22) 통합보안관제 SERCH 구조

추가하여 악성코드 발생 시 이에 대한 관리측면에서 즉각적이며 유연한 실시간적인 대응을 위해서 MPSM에서 취득된 EVENT는 업무환경과 요구사항에 접합한 형태의 맞춤기능형태로 구현되어야 하므로 네트웍 환경에서 API방식으로 설계되어야 함과 동시에 기 기술된 검색 및 능동적인 UI 등의 엔진과 함께 수집된 내용을 정보보안자산과 연계 통합 운용가능한 구



(그림 23) 통합보안관제 MPSM과의 연동 구조

조로 설계되므로서 MPSM에서의 탐지된 악성코드의 이벤트가 해당 인프라에 대한 영향정도와 오탐 및 미탐 기타 잠재적인 위험 여부에 대한 요소로서의 계속적인 탐지 및 분석으로 개념화할 수 있으므로 이러한 방법으로 악성 코드 공격에 대한 즉각적인 사이버 침해 대응을 할 수 있는 설계방안이다. 이에 대해 검증은



(그림 24) 테스트 환경

본 항목 중에 취약점에 대한 탐지여부는 해당 기능상의 차이점과 해석의 차이가 있으므로 검증성 여부에 대해서는 각각의 특징이 있다고 판단되어진다. 다만, 관심 가져야할 항목은 2번 항목 방화벽에 대한 취약점, 9번 항목의 일정 및 REAL-TIME에 의한 취약점 분석 가능여부, 14번 항목의 통합운영가능여부, 11번 항목의 타관리모니터체계와의 연동을 위한 API지원 가능여부 등은 주요 관심사항으로 검토되어야 하는 것을 연구되어진다.

<표 9> 테스트 결과

	Feature	ㅇㅇ사통합취약점분석시스템	I사웹전용취약점분석시스템
1	Find SSH Vulnerabilities	V	X
2	Find Firewall Vulnerabilities	V	X
3	Find common CGI vulnerabilities	V	Partial
4	Find SQL Injection Vulnerabilities	V	V
5	Find Cross Site Scripting Vulnerabilities	V	V
6	Find missing Windows Patches	V	X
7	Find missing Web Server patches	V	Partial
8	Detect insecure form submission	V	V
9	Schedule scans daily/weekly/monthly	V	X
10	Reports in HTML and PDF format	V	V
11	Available as Appliance based solution	V	X
12	Available as Software Based solution	X	V
13	Available as cloud-based solution	V	X
14	Multi-user access control	V	X
15	Distributed Scanning	V	Partial
16	Automated Updates	V	V
17	Find Mail Server Vulnerabilities	V	X
18	Find DNS Server Vulnerabilities	V	X
19	False Positive % (average)	less than 0.01%	~75%
20	Covers Network Layers	4 through 7	Layer 7 only

이에 연구를 수행하면서 추가적으로 논의된 사안으로는

1) 취약점의 탐지 및 분석 대상 로그 및 이벤트에 대해 Non-log, Non- Event에 대한 MPSM 방법론으로 구현방법
2) 취약점탐지 구현절차 및 실시간 구현의 요구되는 기능 및 항목에 대한 연구사항
3) 향후 예상되는 취약점 분석에 대한 오탐 및 미탐에 대한 방법론
4) 일반 네트워크 및 웹 환경 외에 폐쇄망 및 산업 망에 대한 연구된 MPSM 기반으로의 접목여부 등이다

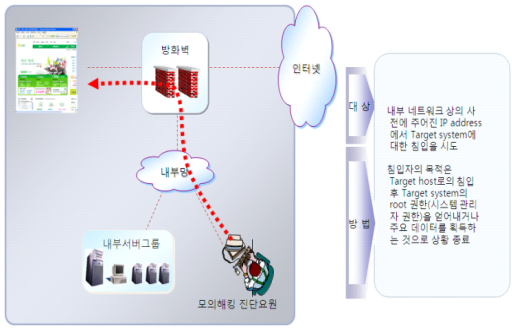
4. 결 론

4.1 연구결과의 요약

본 논문에서는 기존의 단일모드의 취약점점검형태의 기반으로 사이버대응 시 매일 새로이 발견되는 악성코드 증가에 대한 대응 한계와 새로운 공격 방법에 대한 대응방안이 요구되며 기존의 정적(static analysis) 및 동적(dynamic Analysis) 분석패턴연구결과 우회공격과 제로데이 및 un- known에 대한 새로운 악성코드에 대한 대응에 많은 연구를 요구 하게 되는 것으로 결과를 요약하게 된다면.

<기존>

수동 Tool 및 기타 각 영역시스템/네트웍 별도 취약점 점검/분석 도구



<발전 방안>

MPSM-MODULE(시스템+네트웍+OS 취약점점검/분석)+REALTIME → ESM(통합보안관제)

(그림 25) 취약점탐지/분석 프로세스 발전방안

즉 기존의 SINGLE-MODE의 형태에서 EXPLOIT(자동침투)↔DROOPER↔CALL-BACK등의 형태화 되는 구조의 악성코드 공격에 대해 기존의 보고서 및 보고서 형태의 산출물 제공이 아닌 SIEM(Security Information Event& Management: 보안정보 이벤트관리) 또는 ESM/ SIEM(Enterprise Security Management: 통합보안관제)등과 API방식 등의 형태로 연동됨으로서 사이버침해 대응에 대해 즉각적으로 대응할 수 있는 방법론으로 연구한 것으로 <표 10> 검증 및 테스트 분석결과에 대한 산출치다.

<표 10> 검증 및 테스트 분석결과

구분	행위기반분석방법 (WEB. DB. MAIL)	MULTI PROCESSOR SEARCH MODULE
주체	컨설팅업체/ 전문엔지니어	일반관리자/운용자
방식	수동/반자동화	자동화 방식
오진율	2-10%	0.1%미만
네트워크 부하	다소 많음	거의 없음 (전용시스템으로 최적화 환경제공)
스캔방법	단순한 SINGLE - mode방식	MULTIPLE방식
스캔위치	거의외부에서실시	내/외부 모두가능
스캔형태	서버-클라이언트 방식	WEB방식

4.2 연구의 한계

네트워크 및 웹 등의 개방화된 환경에 대한 악성코드에 대한 대응 외에 폐쇄적이고 제한적이며 독립적 환경에서 운용되는 SCADA 시스템에서 절대적으로 요구되는 제로데이 공격 및 Un-Known에 대한 대응키 위해 접목 가능한 측면에서도 연구해야할 과제임과 동시에 모바일 APPLE에 발생가능한 악성코드에 대한 취약점점검 및 분석 대응 논리에 대한 연구과제로 추후에 논고를 해야 할 필요성으로 판단되어진다.

참고문헌

[1] “ADVANCED PERSISTENT THREAT(APT) 공격에 대한 법적 대응방안”, 한국방송통신전파진흥원, 제3호, 2013.

[2] “악성코드 현황 및 탐지기술”, 정보과학학회지, 2012. 1월.

[3] “다양한 취약점점검도구를 이용한 자동화 네트워크 취약점 통합분석시스템설계”, 정보과학회 논문

지, 제14권 제2호, 2008. 4.
[4] “악성코드 유형에 따른 자동화 분석방법론 연구”, 한국정보호보호진흥원, 2011. 5월.
[5] “isc/scada 시스템에 대한 프로코콜 fuzzing 기능 소개”, 한국인터넷진흥원 연구보고서. 2013. 12월.
[6] “취약점 발굴을 위한 프로그램 입력데이터 흐름 분석 연구, 한양대학교 산학협력단, 2013. 11. 29.
[7] 오현식, “apt 전용솔류션의 허와실”, 화산미디어, 네트워크 타임즈, 통권 제225호, 2012. 5. 1.
[8] “고도화된 apt 공격, 전방위적 보안강화가 해결책”, 화산미디어, 네트워크 타임즈, 통권 제221호, 2012. 1월.
[9] API CALL의 단계별 통합분석을 통한 악성코드 탐지 한국정보보호학회 논문집(2012.12)
[10] 김효남, 악성코드탐지를 위한 실시간 통합관리 시스템에 관한 연구, 한국컴퓨터정보학회 하계 학술대회 논문집 제21권 2호(2013.7)
[11] 대규모악성코드 유포동향분석 “주말악성코드탐지대응(전자자료) 한국인터넷 침해대응센타 (2013.6)
[12] 오영근, 배병철, 김은영, 박중길, 실행시간 악성실행코드 탐지시스템 설계 한국정보과학회 학술발표논문집(2008.6) 국가보안기술연구소.
[13] 서정택, 정윤정, 임을규, 김인중, 이철원, 인트라넷 취약점 분석 평가 방법론 연구 한국정보과학회 학술발표논문집(2008.6) 국가보안기술연구소.
[14] 샌드박스 vs 비샌드박스 경쟁 아닌 보완관계 Security Report APT방어기술 집중분석
[15] 천명호, 강혜진, 최종석, 신용태, 취약점분류체계를 통한 연관 취약점 분석 방법연구 숭실대학교 2012년 가을 학술발표논문집(2012.9)
[16} 최영환, 김형천, 홍순좌, Software Security Testing Using Block-Based File Fault Injection 한국정보보호 학회 논문지((2007).
[17] 박남열, 김용민, 우회기법을 이용하는 악성코드 행위기반탐지방법 정보보호학회 논문지 16권3호 (2006.7).
[18] 행정안전부, 주요정보통신기반시설 취약점 분석 평가 기준 (2011)
[19] KAIST, CSRC Malware Trend Analysis Report (2012.6)
[20] 분산서비스 거부 공격도구 Netbot분석보고 한국인터넷진흥원(2008)
[21 API단계별 복합분석을 통한 악성코드탐지 한국정보보호학회논문집(2007.12)

[저 자 소 개]

윤 종 문 (Jong Moon Yoon)

1988년 경희대학교 대학원 산업안전공학 전공(석사)
2013년 경기대학교 산업보안학과 박사과정 수료
2000년 (주)윈스테크넷 총괄본부장
2002년 (주)시큐브 부사장
2008년 (주)웹큐브시큐리티 대표이사
현 (주)세코원 대표이사