윈도우 감사 로그를 활용한 침해사고 모니터링 방안 연구

이현녕
고려대학교 컴퓨터정보통신대학원
e-mail:hyunyung@korea.ac.kr

A study on monitoring method of infringement using Windows audit log

Hyun-Nyung Lee
Graduate School of Computer & Information Technology, Korea University

요 약

네트워크 환경 및 인터넷 활용폭이 다양해지면서 고도화되고 진보적인 보안위협이 발생되고 있으며 발생량도 점차 증가하고 있다. 이에 따라, 네트워크 침입탐지 시스템, 악성행위 탐지 시스템, 웹 방화벽, 안티바이러스 등도 점차 진보된 악성행위를 탐지하는 데 있어 불충분해짐에 따라 기업과 기관 및 보안담당자들은 직관적인 정보를 제공하는 End-Point 로그 수집 및 모니터링으로 변화를 시도하고 있다. 이에 따라, 본 논문에서는 Anti-Virus 및 침입탐지 시스템(IDS), APT, 윈도우 감사로그를 상호 비교하여 보안분석 시스템보다 윈도우 감사로그가 보안위협 및 침해사고를 모니터링하는 면에서 더욱 직관적이고 빠른 대응이 가능하다는 것을 증명한다.

I. 서론

최근의 사이버 침해사고 사례를 보면 드라이브 바이 다운로드, 자바 애플릿 등의 웹을 통한 침해사고, 악성 이메일을 통한 침해사고, 파일서버 등의 서비스를 이용한 침해사고, 저장장치 및 기기를 통한 침해사고 등 다양한 방법을 통해 악성코드 감염 등의 침해사고가 발생하고 있다. 그러나 악성행위들이 대부분 암호화 및 난독화 되어가고 있고 기존의 보안위협을 탐지하는 시스템에서는 고도화되고 진보적으로 변화하는 악성 행위를 탐지하지 못하는 이슈가 발생되고 있으며 증가되고 있는 실정이다.

보안위협을 탐지하는 시스템으로는 침입탐지 시스템, 가상머신을 보유한 악성행위 탐지 시스템, Anti-Virus 등 다양하나 대부분의 시스템별로 위협탐지의 특성이 있다. 따라서 보안조직에서는 SIEM(Security Information and Event Management)을 이용하여 보안 시스템 탐지로그를 수집하고 상호 연계 분석을 진행하고 있다. 다양한 보안위협 탐지/차단 시스템들은 현재 알려진 악성파일 및 공격시도에 대한 내용만을 탐지하고 차단하며 악성파일은 가상 머신에서 분석한다. 침해사고가 발생된 이후에 보안담당자에게 알람이 가는 형태이며 또한 신규 취약점을 통한 Zero-Day Attack 등은 탐지하지 못하는 이슈가 계속적으로 발생되고 있다[1].

이에 윈도우 감사로그를 통한 악성코드 실행 및 감염, 침해사고를 탐지하고 모니터링 하는 방안이 기존의 여러 보안위협 탐지/차단 시스템을 활용하는 것보다 정확성이 높고 대응이 빠르다는 것을 살펴보고자 한다.

II. 연구 배경

윈도우 계열 악성코드에 의한 침해사고에 있어 기업과 기관에서는 다양한 보안 시스템을 활용하여 탐지 및 분석을 한다. 그러나 보안 시스템별로 탐지구간(네트워크/End-Point)과 탐지 특성(시그니처 기반, 가상머신 분석) 등이 다르며 시스템을 구축하는데 많은 비용이 소요되고 각 보안 시스템에서 발생하는 정탐 및 오탐 알람을 일일이 분석하고 대응하기에는 시간적으로도 어려운 상황이다.

보통 악성파일 탐지는 두 가지 방법이 있다. 그 방법으로 의심스러운 실행 파일에서 악성 콘텐츠를 검색해서 탐지하는 정적 분석과 악성 파일의 동작 중에 발생되는 내용을 통한 동적 행위 탐지로 구분하는 방법이다. 상용 Anti-Virus 솔루션들은 대부분 악성 콘텐츠 중심의 정적 분석을 주로 하는 관계로 새롭게 난독화 기술이 적용 된 악성 파일은 신규 정보 업데이트 전까지 탐지하지 못한다. 또한, 가상 머신을 통한 분석 솔루션은 의심 파일이 가상머신에 들어간 후 결과 값이 나오기까지 많은 시간이 걸리며 트래픽이 많으면 많을수록 분석해야 하는 건수도 증가하여 알람을 주는 시간과 대응 시간도 길어진다는 단점이 있다[1].

이를 통해 각 보안분석 시스템, 윈도우 감사로그를 활용하여 상호 비교하였으며 윈도우 감사로그는 SIEM을 통해 모니터링 및 분석을 통하여 정확도가 높고 빠른 대응이 가능하다는 것을 보여준다[2].

III. 연구 내용

보안위협 케이스에 대해 시나리오를 정의 한 후 각 Anti-Virus, 침입탐지 시스템, APT(지능형 지속공격, Advanced Persistent Threat) 탐지 시스템, 윈도우 감사로그 별로 발생 되는 로그의 유/무 및 가상 머신을 통해 분석 후 알람을 주는 시간, 윈도우 감사로그를 상호 비교 한다[3].

윈도우는 독자적인 프로토콜을 채택하고 있으며, 이벤트 뷰어를 통해 로그 검색 및 다운로드가 가능하고 SIEM을 통하여 로그 연계분석 후 모니터링 하는 방법을 연구한다.[4].

3.1 로그 수집

악성 바이너리 파일 실행 시에 발생되고 저장되는 감사 로그를 포함하여 수집하며 수집 되는 감사로그는 [표 1]과 같다.

[표 1] 로그 수집 정보 및 내용

구분	수집 정보	수집 내용
감사 로그	Application	API를 사용하는 응용프로그램의 중요한 이벤트 및 활동 내역을 기록
	Security	시스템 로그온, 파일 접근, 인증, 계정 생성, 권한 사용 등의 내역 기록
	System	시스템 운영과 유지에 관련된 대부분의 정보 등의 내역 기록
	Windows-PowerShell	파워쉘 사용에 따른 내역

3.2 악성파일 탐지 현황

[표 2]에서 보는 것과 같이 침입탐지 시스템은 네트워크 구간에서 탐지 시그니처(문자열)이 존재할 경우 탐지하지만 네트워크 트래픽이 암호화 되었을 경우는 전혀 탐지하지 못하는 것으로 확인되며, Anti-Virus는 End-Point 구간에 설치되므로 기존에 알려진 악성코드에 대해서 탐지는 하지만 신규 악성코드 및 네트워크 구간 트래픽은 별도로 정보 업데이트 전까지 탐지/검사하지 못한다. APT 탐지 시스템 경우에도 네트워크 암호화 트래픽은 별도로 분석하지 못하며 복호화가 가능한 트래픽 및 암호화되지 않은 트래픽에서는 가상 머신을 통해 행위 분석 결과 확인 할 수 있다.

그러나, 윈도우 감사로그에서는 다양한 행위에 대해 로그 저장하므로 네트워크 트래픽에 대한 내용이 없어도 실제적으로 윈도우 OS 단에서 실행되는 파일 정보, 명령어 정보, 계정 정보 등에 대한 다양한 로그를 확인 할 수 있으며 다른 보안분석 시스템들보다 직관적이므로 빠른 대응이 가능하다.

[표 2] 시스템별 탐지 내역

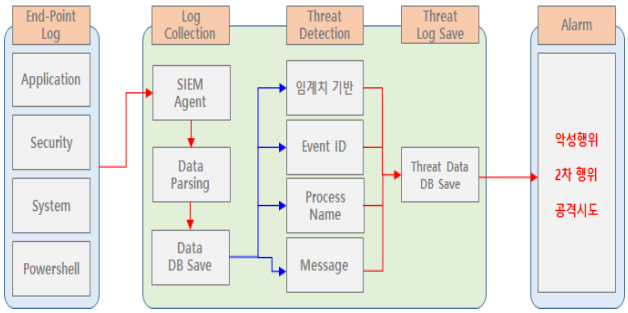
구분	네트워크 구간	End-Point 구간
침입탐지 시스템	△	X
Anti-Virus	X	○
APT	△	X
윈도우 감사로그	X	○

3.3 감사로그 수집 및 저장

윈도우 감사로그는 악의적인 행위시에만 로그를 남기는 것이 아닌, 정상적인 행위에서도 로그를 남

기므로 많은 데이터가 생성되고 저장된다. 그러므로 해당 데이터에 대한 저장이 필요하며 해당 연구에서는 SIEM에 데이터를 저장 및 가공한다.

[그림 1]과 같이 직관적인 감사로그를 통해 데이터 가공이 가능하며 보안위협과 관련된 정보는 SIEM의 메모리상에 상주시켜 위협과 관련된 데이터가 들어왔을 경우 실시간 알람을 받는 형태로 구성한다.

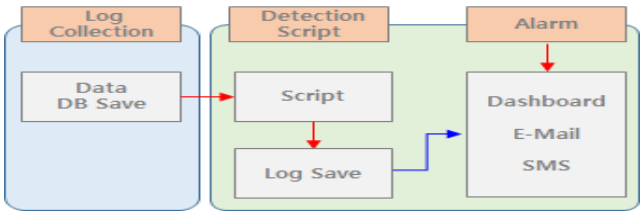


[그림 1] Log 수집 및 위협 탐지 과정

3.4 보안위협 데이터(Log) 검출

저장된 데이터를 활용하여 어떤 정보를 어떻게 이용할 것인지 사전에 정의된 시나리오가 있다면 해당 시나리오에 맞춰 Log Parsing을 진행해야 하며 시나리오를 기반으로 다양하게 위협을 탐지 및 알람을 설정할 수 있다.

보안위협을 탐지하기 위해선 위협이라고 판단되는 정보를 [그림 3]과 같이 스크립트로 작성하여 SIEM에 등록해야 하며, 메모리에 상주시켜야 한다. [그림 2]는 보안위협 탐지 스크립트가 동작하는 과정을 설명한 내용이며, [그림 3]은 보안 위협에 대한 시나리오 내용 스크립트이며 메모리에 상주 시켜 실시간으로 모니터링 및 분석이 가능하다는 것을 보여준다.



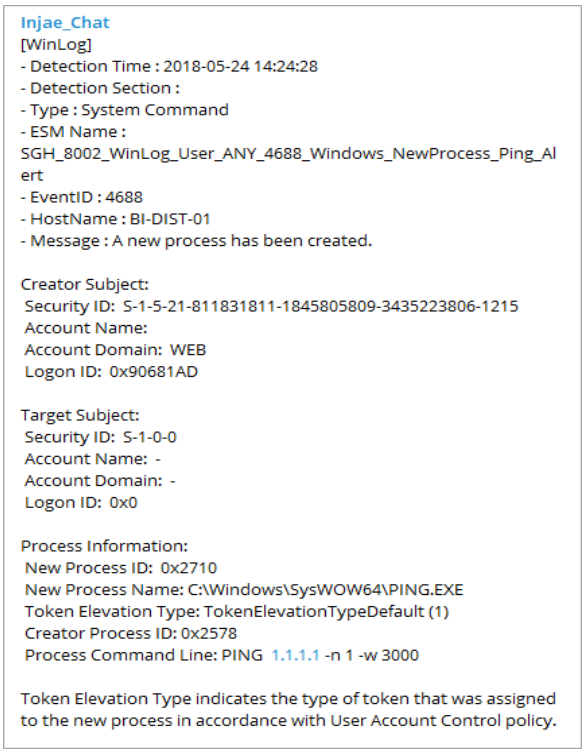
[그림 2] 시나리오 기반 보안위협 탐지 과정

```
eval esm =
case(
event_id == 4688 and lower(message) == "*winrs.exe*",
"SGH_8001_WinLog_User_ANY_4688_Windows_NewProcess_WinRs_Alert",

event_id == 4688 and lower(message) == "*ping.exe*",
"SGH_8002_WinLog_User_ANY_4688_Windows_NewProcess_Ping_Alert",

event_id == 4688 and lower(message) == "*quser*",
"SGH_8003_WinLog_User_ANY_4688_Windows_NewProcess_Quser_Alert",

event_id == 4688 and lower(message) == "*psexec*" and (message != "*hcyoo_dc*"),
"SGH_8004_WinLog_User_ANY_4688_Windows_NewProcess_Psexec_Alert",

event_id == 4688 and lower(message) == "*psexesvc.exe*",
"SGH_8005_WinLog_User_ANY_4688_Windows_NewProcess_Psexesvc_Alert",

event_id == 4688 and lower(message) == "*net.exe*" and lower(message) == "* use *",
"SGH_8006_WinLog_User_ANY_4688_Windows_NewProcess_Net_Use_Alert",

| search isnotnull(esm)

| lookup kafka_win_log esm output type, device, hazard, severity
| fields _time, hazard, esm, device, type, event_id, host, message, tags

| eval key = concat(host, "=", esm)

| serial
[
evtctxadd topic="kafka_win_log" key=key timeout=5m maxrows=0 isnotnull(key)
| eval evt_count = evtctxget("kafka_win_log",key, "counter")
]

| search evt_count == 1

| import esml_server_winlog
```

[그림 3] 시나리오 기반 탐지 스크립트

3.5 보안위협 실시간 알람 (텔레그램 메신저)

[그림 4]와 같이 SIEM의 보안위협 로그를 텔레그램 API를 통해 메신저 연동 가능하며 데스크탑 PC, 태블릿, 휴대전화 등에서 자유롭고 빠르게 탐지된 보안위협 로그의 모니터링이 가능하다.



[그림 4] SIEM 대시보드

IV. 연구 결과

보안분석 시스템과 윈도우 감사로그를 비교한 결과, 보안분석 시스템이 알람을 주는 경우는 대부분 사전에 정의된(알려진) 공격들이 대부분이었으며, 암호화 된 네트워크 구성에서는 탐지 및 알람을 주지 못하는 경우가 많았다. 그에 반해, 윈도우 감사로그는 OS 상에서 이루어지는 행위들에 대해 로그로 모두 저장하므로 분석시간 면이나 암호화된 네트워크 환경에서 모두 효율성이 높다는 결론을 보였다.

[표 3]과 같이, 20일 평균 저장되는 로그를 바탕으로 효율성을 비교 검증 결과, 윈도우 감사로그는 저장되는 수치가 많은 반면 로그에서 볼 수 있는 내용이 직관적이므로 분석시간이 매우 짧고 대응 또한 효율적이라는 것을 알 수 있다.

[표 3] 탐지로그 및 분석 건수 (시간)

Log Type	Input Data	Analysis Case	Responsetime (1건/min)
IDS	90,465	248	41h 20m (10min)
Anti-Virus	14,224	5	10h (120min)
APT	184	9	9h (60min)
윈도우 감사로그	1,227,091	107	5h 21m (3min)

저장 데이터 대비 분석 케이스는 IDS가 가장 많았으며 Anti-Virus가 적었다. 1건당 분석시간 소요 기준으로는 윈도우 감사로그가 3분으로 가장 짧았고 Anti-Virus 120분으로 길었다. 연구결과, 윈도우 감사로그가 저장되는 로그가 제일 많았지만 분석 케이스 및 분석에 걸리는 시간은 저장로그 수치 대비 가장 효율적인 것으로 확인되었다.

V. 결론

본 연구논문에서는 대량의 윈도우 감사로그를 바탕으로 악의적인 보안위협에 대한 로그를 실시간 탐지 및 대응 할 수 있는 방안에 대해 제시하였다. 더 좋은 방법은 윈도우 감사로그만 보는 것보다 이기종 보안분석 시스템을 함께 로그 분석하는 것이 효율성 면에서 더욱 좋을 수 있으므로 여러 가지 시나리오에 대해 파악하고 만드는 것이 중요하다.

또한, 침해사고 피해를 입고 대응하는 것보다는 보안 위협을 사전에 탐지하고 분석가가 빠른 대응을 할 수 있도록 우선순위가 높은 로그를 경고하는 보안 로그 분석 프레임 워크를 사전에 만들고 제공해야 한다[5].

향후 본 논문에서 연구한 내용과 더불어 이기종 보안 시스템 및 서버로그, 웹 로그 등을 활용하여 보안위협과 침해사고 모니터링 및 분석에 있어 성능과 효율성 등을 추가 분석하는 연구를 진행할 예정이다.

[참고문헌]

[1] Konstantin Berlin, David Slater, Joshua Saxe, “Malicious Behavior Detection using Windows Audit Logs”,AISec '15,1,2015.10

[2] 바이러스토탈 (Virustotal) (https://www.virustotal.com)

[3] 지능형 지속 공격(APT) (https://ko.wikipedia.org/wiki/지능형_지속_공격)

[4] 김완집, 염흥열,“이기종 로그에 대한 통합관리와 IT 컴플라이언스 준수”, 한국정보보호학회 ,제 20권 5호,3,2010.10

[5] Zhou Li, Alina Oprea,“Operational security log analytics for enterprise breach detection”, IEEE Cybersecurity Development Conference,8,2016