ELK Stack과 Sysmon을 이용한 EDR 플랫폼 연구

신현창* · 공승준 · 오명호 · 이동휘

동신대학교

EDR platform construction using ELK Stack and Sysmon

Hyun-chang Shin* · Seung-Jun Kong · Myung-ho Oh · Dong-hwi Lee

Dongshin University

E-mail : tlsgusckd124@gmail.com / szkong@naver.com / dhajd444@gmail.com / dhclub@dsu.ac.kr

요 약

IT 기술의 발전과 함께 사이버 범죄는 정교해지고 지능화되고 있다. 특히 APT공격(지능형 지속 공격) 과정에서 사용되는 BackDoor의 경우 자신이 공격자에게 피해를 받았다는 사실조차 모르는 경우가 많고 사전 탐지가 힘들며 발견 전까지는 지속적인 피해를 받기 때문에 악성 행위 탐지와 침해 대응이 매우 중요하다. 본 논문에서는 오픈소스 기반 분석 솔루션인 ELK Stack과 Sysmon을 이용하여 엔드포인트 환경에서 실시간으로 로그를 수집, 저장, 분석 및 시각화하여 실시간으로 악성행위에 대한 모니터링 및 분석과 대응이 가능한 EDR 플랫폼 구축을 목표로 한다.

ABSTRACT

With the development of IT technology, cybercrime is becoming sophisticated and intelligent. In particular, in the case of BackDoor, which is used in the APT attack (intelligent continuous attack), it is very important to detect malicious behavior and respond to infringement because it is often unaware that it has been damaged by an attacker. This paper aims to build an EDR platform that can monitor, analyze, and respond to malicious behavior in real time by collecting, storing, analyzing, and visualizing logs in an endpoint environment in real time using open source-based analysis solutions ELK Stack and Sysmon.

키워드

EDR, ELK Stack, Sysmon, Backdoor, 악성코드

1. 서 론

IT 기술의 발전으로 정보보호에 대한 중요성이 굉장히 부각됨에 따라 관련 분야 및 기술들도 꾸준한 성장을 이루었다. 그러나 악성코드 역시 이에 맞춰 정교화되고 지능화 되어가고 있으며 이로 인한 피해사례는 지속적으로 늘어나고 있는 추세이다. KISA(한국 인터넷 진흥원)의 분석 보고서에 따르면 2021년 한 해 동안 탐지된 악성코드는 5005건으로 2020년 대비 49%(3350건) 증가하였으며 악성코드의 종류와 사용된 기술들이 모두 다양하다는 점에서 앞으로도 발전된 기술들이 내포된 새로운 종류의 악성코드들이 등장할 것이라 판단된다[1]. 이러한 악성코드들의 경우 미리 입력시켜둔 패턴을 기준으로 악성코드를 탐지하는 시그니처 기반 탐지 방법으로는 탐지가 힘들다. 악성코드의 패턴을 조금만 바꿔도 정보보호 장비를 손쉽게 우회할 수 있기 때문이다. 높은 수준의 기술과 충분한 자원을 보유한 공격자가 목표를 설정하고 장기간에 걸쳐 지속적인 침투를 시도하여 특정 IT 인프라를 장악하는 APT(Advanced Persistent Threa) 공격과 새로운 패턴의 공격, 혹은 발견된 취약점에 대한 패치가 이뤄지지 않은 제로데이(Zero-day) 공격이 대표적인 예이다. 고도화된 공격 방식에 대응하려면 보안 위협의 탐지 영역을 네트워크 영역에서 실제로 보안 위협이 발생하는 엔드포인트(End Point) 단으로 확장할 필요성이 있다. 이러한 엔드포인트 보안중 하나인 EDR(Endpoint Detection and Response)은 지속적 주시와 대응에 초점을 두며 원

* corresponding author

천적인 예방보다는 수상한 행동이 발생했을 경우에 대한 빠른 탐지와 초기 조치를 중요시한다. 클라이언트에 설치된 에이전트는 발생하는 모든 활동을 실시간으로 모니터링하고 데이터를 수집하여 중앙 서버에 전송한다. 수집된 데이터에서 의심스러운 행동이나 이상징후가 탐지될 시 해당 행위에 대한 대응 및 보안 담당자에게 알림으로써 위협에 대한 초기 대응을 신속하게 할 수 있도록 한다[2][3].

본 연구에서는 ELK Stack과 Sysmon을 사용하여 엔드포인트 환경에서 발생하는 로그들을 실시간으로 수집하고 수집된 엔드포인트 데이터를 분석하여 사용자별 행동 패턴을 파악한 뒤 이와 다른 패턴이 발생했을 경우 위협 가능성이 있는 행위로 판단하여 보안 위협을 탐지하고 이를 시각화하여 보안 담당자들이 보다 쉽게 보안 위협을 파악할 수 있는 EDR 플랫폼 프로토 타입 구축을 목표로 둔다.

본 논문의 사용 기술 설명, 환경 구축, 가상 침해사고 시나리오, 악성 및 이상 행위 탐지 로그 분석, 결론 및 향후 연구로 이어진다.

2. 제안기술

2-1 ELK Stack

ELK Stack은 Elasticsearch, Logstash 및 Kibana 세 개의 오픈 프로젝트를 합친 ELK에 Beats를 추가한 솔루션이다. 그림1. 은 세가지 모듈의 각 기능을 설명해주며 Elasticsearch는 분석 및 저장 기능, Logstash 는 수집 및 재가공 , Kibana는 시각화 탐색 및 실시간 분석을 담당하며, 이를 통해 접근성과 편리성을 갖춘 데이터 분석을 제공 한다.

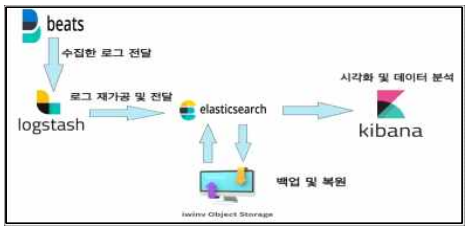

그림 1. ELK Stack 구조

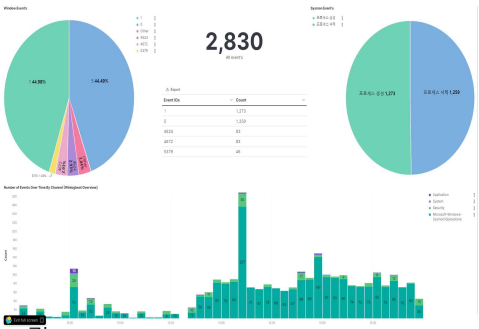

그림 2. Kibana Main Dashboard

2-2 Winlogbeat

Winlogbeat는 windows 환경에서 사용되는 경량 이벤트 로그 수집기다. windows 이벤트 로그를 디스크에 스풀링하여 파이프라인이 데이터 요소를 수집하며 Sysmon의 로그를 통해 수집된 데이터를 Logstash로 전송하여 Kibana로 시각화가 가능하기 때문에 Sysmon 및 ELK Stack과 함께 사용했다.

2-3 Sysmon

Sysmon은 Sysinternals에서 내놓은 도구로 기본 윈도우 이벤트 로그와 마찬가지인 시스템 모니터링 툴이다. 기존 윈도우 이벤트 로그의 한계가 있는 프로세스 생성, 네트워크 연결등을 이벤트 화 시켜주는 역할을 수행한다. Sysmon에서 제공하는 로그 이벤트 중에서 특히, 파일·프로세스·WMI·레지스트리 이벤트를 이용하여 프롬프트 등에 의한 악성코드 감염이나 정상적인 윈도우 명령어 사용을 통한 네트워크 탐색 및 내부 프로세스·파일 목록 검색 등 Lateral Movement를 탐지할 수 있다.

2-3 EDR (Endpoint Detection and response)

엔드포인트 탐지 및 대응(EDR)은 PC, 노트북 등 네트워크의 모든 엔드포인트 영역에서 지속적으로 모니터링 하고 데이터를 수집한 뒤 이를 실시간으로 분석하여 보안 위협에 대한 탐지 및 분석, 대응할 수 있게 하는 엔드포인트 보안 방법이다.

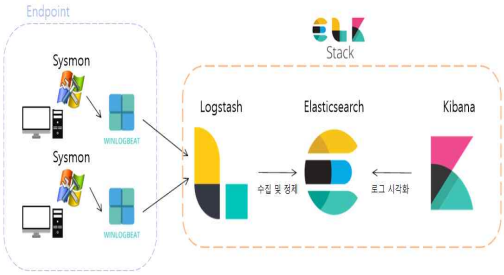

그림 3. EDR 플랫폼 구성도

본 논문에서는 ELK Stack과 Sysmon을 활용하여 (그림 2)와 같은 환경을 구성한 뒤 엔드포인트에서 발생하는 로그들을 수집하고 (그림 3)의 과정을 거쳐 (그림 4)의 Main DashBoard를 통해 분석한다.

3. 제안기술 평가

3-1 엔드포인트 공격

엔드포인트 환경은 Embeded PC를 사용하여 다중 환경을 구성하였다. Embeded PC의 사양은 (표 1)과 같으며 다른 종류의 악성코드를 실행시켜 발생하는 로그들에 대해 수집 및 분석을 진행했다.

표 1. Embeded PC Specification

Embeded PC Specification	
OS	Windows10
CPU	Intel(R) Core(TM) i5-4210U @ 1.70GHz 2.40GHz
RAM	8.00 GB
System	x64 bit

다중 엔드포인트 환경에서 실행할 악성코드는 두 종류이며 각각 BackDoor와 자동 화면 캡쳐 악성코드이다. BackDoor 악성코드는 dllshot.exe 라는 이름으로 Kali Linux의 Metasploit을 사용하여 제작하였고 자동 화면 캡쳐 악성코드는 nircmd의 화면 캡처 기능과 cmd 명령어를 함께 사용하여 제작했다.

3-2 Backdoor

엔드포인트 환경에서 Backdoor인 dllhost.exe를 실행시켰을 때 공격자의 msfconsole에서는 해당 엔드포인트 환경과의 세션 연결 결과를 확인할 수 있었고 이러한 로그는 Sysmon을 통해 수집되어 Kibana의 Discover 부분에서도 확인이 가능하였다. (그림 5.) 와 같이 Time Filtering을 통하여 악성코드가 실행되었던 시간대 전, 후 30분을 DashBoard로 출력하였을 때 해당 시간대에서 Sysmon 로그 수집이 활발하게 이뤄짐을 알 수 있었으며 이를 통해 해당 엔드포인트 환경에서 비정상적인 행위가 일어나고 있음을 파악하였다.

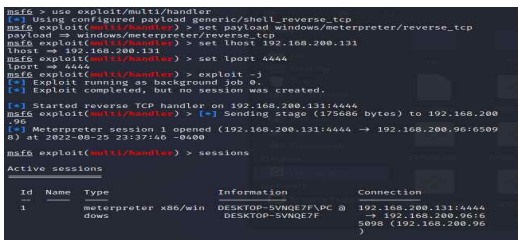

그림 4. BackDoor 공격 실행

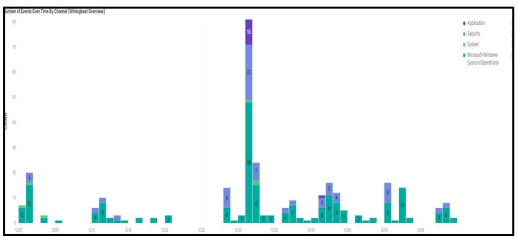

그림 5. Kibana 이용 BackDoor Log 시각화

3-3 자동 화면 캡처 악성코드

자동 화면 캡쳐 악성코드는 nircmd의 화면 캡쳐 명령어와 cmd 명령어를 같이 사용하여 .bat 파일로 제작하였다. 해당 bat 파일을 실행시키면 nircmd의 savescreenshot 명령어를 사용하여 10초에 한 번씩 화면이 캡쳐되게 만들었으며 nircmd가 윈도우 커맨드 라인(CMD 또는 PowerShell)에서 윈도우를 제어할 수 있도록 도움을 주는 라이브러리라는 특성 때문에 Window Defender나 기타 백신에서는 잡히지 않는다.

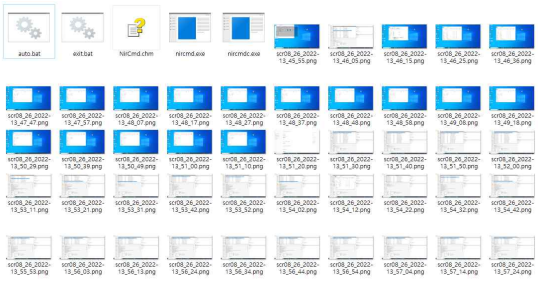

그림 6. nircmd Screenshot

nircmd는 dll 형식으로 돌아가며 10초에 한 번씩 명령어가 실행될 때마다 Sysmon에서는 dllhost.exe로 로그가 생성된다. Sysmon의 1번 evnet id는 Process Create로 화면이 캡쳐될 때 발생하는 로그이고 5번 event id는 Process Terminate로 화면 캡쳐가 종료될 때 발생하는 로그이다. nircmd가 종료되기 전까지는 해당 로그가 10초 간격으로 계속해서 발생하며 nircmd가 실행된 시점에서부터 종료될 때까지 발생한 다량의 Sysmon Log들이 다른 시간대보다 월등히 많은 것을 Kibana로 확인할 수 있었다. (그림 7)과 같이 엔드포인트에서 nircmd가 실행되기 전과 후의 평균 로그 발생량이 차이가 많이 나는 것을 확인할 수 있다.

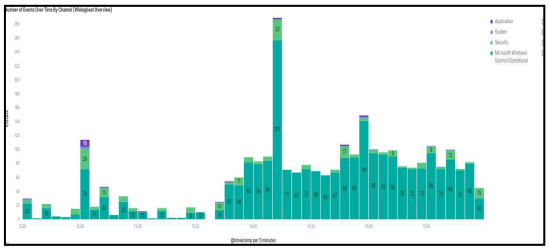

그림 7. Kibana 이용 nircmd Log 시각화

상용 정보보호 솔루션인 UTM을 사용하여 EDR 플랫폼과의 탐지 결과를 비교해보았을 때, 표 2.와 같이 엔드포인트 영역 탐지 부분에서 차이가 있었다. 가장 큰 차이점은 발생하는 로그와 이벤트에 대해 사용자의 일반적 상태를 정립할 수 있는지에 대한 부분이었다. 신뢰된 사용자에서 발생하는 로그인 것으로만 판단하는 UTM과 다르게 EDR 플랫

폼에서는 로그 발생률, 발생 빈도를 시각화함으로써 해당 사용자에 대한 일반적 상태를 정립할 수 있었고 이를 통해 특정 사용자에게서 발생한 보안 위협에 대해 일반적 상태를 벗어났을 경우 보안 위협 가능성이 있는지에 대한 여부를 판단할 수 있었다.

표 2. UTM과 EDR 플랫폼 탐지 결과

EDR Platform		UTM	
엔드포인트 영역		엔드포인트 영역	
Backdoor	O	Backdoor	X
nircmd	O	nircmd	X

4. 결 론

본 논문에서는 ELK Stack과 Sysmon을 이용한 EDR 플랫폼을 연구하고 프로토타입을 구축해보았다. 엔드포인트 환경을 구성한 뒤 Sysmon을 설치해 발생하는 모든 로그들을 수집하고 수집된 로그를 기반으로 각각의 사용자에 대한 일반적 상태를 정의한 뒤 이를 크게 벗어나는 패턴이 발생했을 경우 보안 위협 가능성이 있는 행위로써 해당 위협을 탐지하고자 하였다. 구축한 프로토타입은 상용 정보보호 솔루션인 UTM(Unified Threat Management)과의 영역별 탐지 여부를 비교하여 EDR 플랫폼의 필요성을 증명하였다. APT 공격과 피싱 메일 등 특정 대상을 목표로 한 공격의 경우 엔드포인트 영역에서부터 해킹이 시작되기 때문에 이를 사전에 탐지하고 초기 대응하는 것이 중요하다. 따라서 본 연구에서 제시한 EDR 플랫폼과 같은 보안 위협 탐지 환경을 구축한다면 엔드포인트 영역에서 발생하는 보안 위협에 대해 신속하고 효율적으로 대응 및 조치가 가능할 것이며 시그니처 기반 탐지 방법으로 탐지가 어려운 공격이나 신, 변종 악성코드들에 대해서도 대응이 가능할 것이다.

Acknowledgement

본 과제(결과물)는 2022년 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다. (NRF-1345341782)

References

[1] KISA. Cyber Threat Trend Report for the First Half of 2021. [Internet]. Available : https://www.kisa.or.kr/20205/form?postSeq=1016&page=1#fnPostAttachDownload

[2] Cholong Yoo, Pilsung Kang, “A Study on Threat Detection based on User Behavior Model Using System Event Logs of Endpoint Security Solution,” *Journal of the Korean Institute of Industrial Engineers,* Vol. 46, No. 6, pp. 637-649, Dec. 2020.

[3] Jeong-Hoon Hyun, Hyoung-Joong Kim, “Security Operation Implementation through Big Data Analysis by Using Open Source ELK Stack,” *Journal of Digital Contents Society*, Vol. 19, No. 1, pp. 181-191, Jan. 2018.

[4] Jeon Sang June, Yun Seong Yul, Kim Jeong Ho, “Design and Evaluation Security Control Iconology for Big Data Processing,” *Journal of Platform Technology*, Vol. 8, No. 4, pp. 38-46, Dec. 2020.

[5] Yongjun Kim, Taeshik Shon, “Cyber-Threat Detection of ICS Using Sysmon and ELK,” *Journal of The Korea Institute of Information Security & Cryptology*, Vol. 29, No. 2, pp. 331-346, Apr. 2019.