The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 21, No. 4, pp.15-23, Aug. 31, 2021. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2021.21.4.15
JIIBC 2021-4-3

우회 원격공격의 위협탐지를 위한 위협 헌팅 모델 연구

A study on the threat hunting model for threat detection of circumvent connection remote attack

김인환*, 류호찬**, 조경민**, 전병국***

Inhwan Kim*, Hochan Ryu**, Kyeongmin Jo**, Byungkook Jeon***

요 약 대부분의 해킹 과정에서는 장기간에 걸쳐 내부에 침입하고 목적 달성을 위해 우회접속을 이용한 외부와 통신을 시도한다. 고도화되고 지능화된 사이버 위협에 대응하는 연구는 주로 시그니처 기반의 탐지 및 차단 방법으로 진행되었으나, 최근에는 위협 헌팅 방법으로 확장되었다. 조직적인 해킹그룹의 공격은 장기간에 걸쳐 지능형 지속 공격이면서, 우회 원격 공격이 대부분을 차지한다. 그러나 지능화된 인지 기술을 활용한 침입 탐지 시스템에서도 기존의 침입 형태에만 탐지성능을 발휘할 뿐이다. 따라서, 표적형 우회 원격 공격에 대한 대응은 기존의 탐지 방법과 위협 헌팅 방법으로도 여전히 한계점이 있다. 본 논문에서는 이러한 한계점을 극복하기 위해 조직적인 해킹그룹의 표적형 우회 원격 공격 위협을 탐지할 수 있는 모델을 제안한다. 이 모델은 우회 원격 접속자의 원점 IP 확인 방법을 적용한 위협 헌팅 절차를 설계하였고, 실제 국방 정보체계 환경에서 제안한 방법을 구현하여 유효성을 검증하였다.

Abstract In most hacking attacks, hackers intrudes inside for a long period of time and attempts to communicate with the outside using a circumvent connection to achieve purpose. research in response to advanced and intelligent cyber threats has been mainly conducted with signature-based detection and blocking methods, but recently it has been extended to threat hunting methods. attacks from organized hacking groups are advanced persistent attacks over a long period of time, and bypass remote attacks account for the majority. however, even in the intrusion detection system using intelligent recognition technology, it only shows detection performance of the existing intrusion status. therefore, countermeasures against targeted bypass rwjqthrwkemote attacks still have limitations with existing detection methods and threat hunting methods. in this paper, to overcome theses limitations, we propose a model that can detect the targeted circumvent connection remote attack threat of an organized hacking group. this model designed a threat hunting process model that applied the method of verifying the origin IP of the remote circumvent connection, and verified the effectiveness by implementing the proposed method in actual defense information system environment.

Key Words : VPN Detection, Circumvent Connection, threat hunting, Advanced Persistent Threat, threat detection

*정회원, 강릉원주대 소프트웨어공학과
**준회원, Defense Integrated Data Center
접수일자 2021년 6월 28일, 수정완료 2021년 7월 28일
게재확정일자 2021년 8월 6일

Received: 28 June, 2021 / Revised: 28 July, 2021 /
Accepted: 6 August, 2021
***Corresponding Author: jeonbk@gwnu.ac.kr
Dept. of Software, GangneungWonju Nat'l University, Korea

Ⅰ. 서 론

VPN(Virtual Private Network) 서비스는 암호화된 보안 터널을 제공하여 실제 트래픽을 숨기는 기능을 제공하는 특징이 있다. [1-4,19] 이와 같은 VPN 특징으로 인해 자택이나 해외 등 원격지에서 접속하여 업무를 수행할 수 있지만, 해커(hacker)에게는 유용한 우회접속 수단으로 활용된다. '미국의 대기업에는 두부류가 있다. 해킹을 당한 기업과 아직도 해킹당한 사실을 알아차리지 못한 기업이다.'[1]고 언급된 바와 같이 해킹의 위협으로부터 상시 노출되어 있다. [5]

해결 방안으로는 주로 시그니처 기반의 탐지 및 차단하는 방법이었으나, 최근에는 내부에 존재하지만 알려지지 않는 위협을 찾는 위협 헌팅 방법으로 확장되어왔다. 그러나 국가급에서 조직적으로 지원하는 해킹그룹의 공격은 장기간에 걸쳐 지능형 지속 공격(APT : Advanced Persistent Threat)이면서, 우회 원격 공격이 대부분을 차지한다. 이에 상응하는 표적형 사이버 위협을 탐지하기 위한 지능화된 침입 인지기술 등이 연구되었다. [6,7] 그러나 지능형 인지기술을 활용한 침입 탐지 시스템에서도 기존의 침입 형태에만 탐지성능을 제공할 뿐이다. 따라서, 표적형 우회 원격 공격에 대한 대응은 기존의 탐지 방법과 내부를 대상으로 한 위협 헌팅 방법으로도 여전히 한계점이 있다.

본 논문에서는 이러한 한계점을 극복하기 위해 조직적인 해킹그룹의 표적형 우회 원격 공격 위협을 탐지할 수 있는 모델을 제안한다. 제안된 모델은 사이버 킬체인 모델에서 제시된 사이버 정찰이나 전달 및 명령·제어 단계에 필수 수단인 외부와 통신 중에서 우회 접속자를 식별하고 내부 대상 위협 헌팅 방법과 연결하여 위협에 대응하는 특징이 있다. [8-10] 따라서, 우선 내·외부간 연결을 시도하는 VPN 우회 접속자 확인 방법을 적용하여 목표와 대상을 명확히 한다. 그리고 내부 대상 위협 헌팅을 수행하여 표적형 우회 원격 공격 위협탐지 모델을 설계하고 검증한다.

본 논문의 구성으로 2장에서는 우회 접속자 원점 IP 확인 방법 및 사이버 위협 헌팅 등 관련 연구에 대해 알아본다. 3장에서는 우회 접속자 원점 IP 확인 방법을 적용한 조직적인 해킹그룹의 공격 위협에 대응한 위협 헌팅 모델을 제안한다. 4장에서는 실험을 통해 제안한 위협 헌팅 모델의 유효성을 검증하였다. 마지막으로 결론 및 향후 연구 방향을 논한다.

1) 제임스 코미 전 미국 연방수사국장, 2014.10.5.

Ⅱ. 관련 연구

1. 내부에 알려지지 않은 위협

방어 관점에서는 사이버 위협을 알려진 위협과 알려지지 않은 위협으로 구분한다. 알려진 위협은 공격자의 무기 즉 악성코드가 노출되고 분석되어 백신 등 정보보호체계에 의해 방어된다. 이는 정보보호체계의 경계선 방어에서 차단 및 탐지되고, 내부에서는 백신으로 치료하는 방법이다. 이러한 악성코드는 백신에 의한 치료가 가능하여 일반적으로 바이러스라고 통칭한다. 반면, 알려지지 않는 위협은 공격자의 악성코드가 노출되지 않아서 정보보호체계에 탐지, 차단 및 치료되지 않는 멀웨어[2] (malware)가 대표적이다. 이러한 알려지지 않은 위협은 그림 1과 같이 록히드 마틴의 사이버 킬체인 모델 4단계(악용) 이상에서 활동하고 있으나 식별되지 않는 것으로 볼 수 있다. [8]

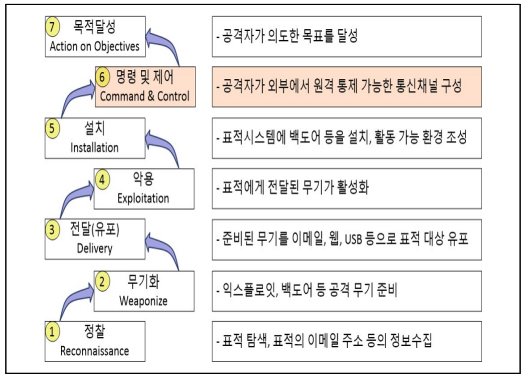

그림 1. 록히드 마틴의 사이버 킬체인 공격모델
Fig. 1. Lockheed Martin's Cyber Kill Chain Attack Model

이렇게 식별되지 않는 이유는 해커의 활동 흔적을 식별하는 어려움을 표현하고 있는 그림 2의 피라미드에서 알 수 있듯이 조직적인 해킹 그룹에서는 정보보호체계를 회피할 수 있는 도구(무기)와 공격 전술, 기술 및 절차(TTPs : Tactics Techniques and Procedures)를 사용하고 있는 사실의 반증이기도 하다. [11-12]

2) 컴퓨터 및 네트워크에 유해한 영향을 끼치는 모든 소프트웨어의 총칭으로 바이러스, 랜섬웨어, 트로이목마 등의 다양한 종류가 있음(위키백과, wikipedia.org)

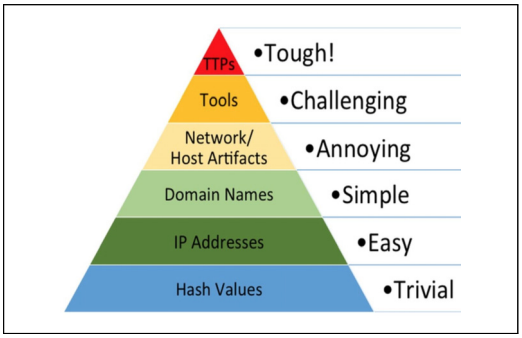

그림 2. 고통의 피리미드 [11]
Fig. 2. Pyramid of Pain [11]

또한, 그림 2의 피라미드는 지표 유형 간의 관계와 해당 지표를 거부할 수 있을 때 공격자에게 줄 수 있는 고통의 정도를 높이와 색상으로 보여주고 있다. 따라서 내부에 존재하지만 알려지지 않은 위협을 찾는 위협 헌팅이 유용한 방어 방법이다. 더욱이 공격자가 사이버 킬체인 6단계(명령 및 제어)에 성공하기 이전에 공격징후를 탐지하여 차단하는 활동이 성공적인 방어의 핵심 요인이다.

2. 우회 접속자 원점 IP 확인

조직적인 해킹그룹은 자신의 접속 IP 노출을 회피할 목적으로 숨기거나 변형하는 우회접속 방법을 이용한다. Kim 등은 VPN 등 프락시(proxy)를 통한 우회접속에 관한 체계적인 모델링과 원점 IP 확인 방법을 제안하고 구현하였다. [13] 특히 VPN을 이용한 공격자의 원점 IP를 식별하기 위해 접속 과정을 모델링 하였다. 여기서 공격자의 통신행위는 암호화된 VPN 터널 구간(공격자 PC와 VPN 서버 간 통신)에 의해 중간에 가로채더라도 노출되지 않는다. 그리고 공격자의 원점 IP는 VPN 서버 주소로 변환되어 피해자의 서버에서 확인할 수 없다.

조직적인 해킹그룹의 공격자는 이러한 우회접속 방법을 이용하여 자신의 정체를 숨기고 사이버 정보 탈취나 파괴 등의 목적을 달성하는 수단으로 활용한다. 그러나 방어자 관점에서는 VPN을 이용한 우회 접속자 모두를 의도적인 악성 행위 수행자로 분류하는 것은 현실적으로 어려운 실정이다. 그래서 승인된 VPN 접속자의 승인된 권한의 범위와 업무처리 절차에 대한 관리가 요구된다. 이러한 조치에도 불구하고 조직적인 해킹그룹이 수행하는 VPN 등의 우회 원격 공격을 식별하는 것은 현실적으로 매우 제한된다. 따라서, 우회 접속자 원점 IP 확인 방법과 연계된 적극적인 위협탐지 방안 연구가 절실히 필요하다.

3. 내부에 존재하는 위협을 찾는 위협 헌팅

위협 헌팅은 내부에 탐지하지 못하는 위협이 존재한다고 가정하고 이를 능동적으로 찾으려는 활동 과정이다. 조직적인 해킹그룹의 공격에는 장기간에 걸쳐서 은밀하게 정보보호체계를 우회하여 진행되기 때문에 사용자는 해킹을 당하고 있다는 사실 자체를 모르고 있는 경우가 대다수이다.

최근 발표된 Fireeye Mandiant 보고서에 의하면 해킹 공격의 세계 평균 지속시간 중앙값이 56일로 발표되었다. [14] 이는 실제 침해 시작 이후 해킹을 당했다는 사실을 알아내기까지 소요된 기간을 의미한다. 더구나 내부에 침투된 위협을 조기에 식별하는 것이 어렵다는 사실을 나타내고 있다.

위협 헌팅 연구로서 Sqrrl사는 위협 헌팅 성숙도 수준 모델과 위협 헌팅 절차로 헌팅 루프를 제시하고 있다. [9] 또한, 위협 헌팅을 수행하는 방법으로 위협 헌팅 성숙도 수준과 헌팅 루프 단계를 매트릭스로 제시하였다. Gunter와 Seitz는 위협 헌팅 수행을 위한 실용적인 모델을 제안하였다. [10] 수행 절차는 목적, 범위, 도구, 계획검토, 실행, 피드백의 6단계 구성으로 제시하였다. 제시된 모델의 관점은 위협 헌팅을 분석가 중심의 사전 예방적 절차를 정의하고 있다. 또한, 피드백에서는 이전에 수행된 단계에 대해 분석하고 영향성을 검토하여 개선 요소를 반영하여 반복적으로 수행한다. [10] 그리고 R. Stillions은 0~8단계까지 위협탐지 성숙도 수준 모델(DML, Detection Maturity Level Model)을 제안하였다. [15] S. Bromander는 의미론적 사이버 위협 모델을 제시하여 사이버 위협 분류와 특징 추출 등 사이버 보안 위협과 공격의 의미론적 접근을 설명하였다. [16]

알려지지 않는 위협을 찾는 위협 헌팅은 기관이나 기업에서 내부에 존재하는 위협을 탐색하는 지속적이며 체계적인 활동 과정이다. 이를 위해서는 위협 헌터와 탐지, 분석, 대응 및 수단적인 도구 등이 필수적인 충족 조건으로 전제되어야 한다. [9,10] Ryu 등은 국방 정보체계 특성을 고려하여 가설 생성, 정보수집 및 TTPs 추론 그리고 검증 및 피드백의 3단계 위협 헌팅 적용 방안을 제안하였다. [17] 제안된 위협 헌팅 적용 결과는 실제 국방 환경에서 실험하여 유효성을 검증하였다.

방어자 관점에서는 외부에서 우회 원격 공격으로 대량의 기밀자료가 탈취되거나 정보체계 자산 파괴 등의 피해가 가장 심각한 상황이다. 따라서, 조직적인 해킹그룹에서 정보보호체계를 우회한 원격 공격 위협을 탐지 및 대응하기 위한 실용적이고 유용한 방안이 요구되고 있

다. 본 논문에서는 조직적인 해킹그룹의 우회 원격 공격 위협에 대응할 수 있는 유용한 적용 모델을 제안한다.

Ⅲ. 표적형 우회 원격 공격에 대응한 위협 헌팅 절차 모델

본 논문에서는 내부에 존재하지만 탐지해 내지 못하는 위협을 찾는 능동적인 탐지 방법인 위협 헌팅에 외부로부터 은밀한 우회 원격 공격자의 원점 IP를 식별하는 방법을 결합한 위협 헌팅 적용 모델을 제안한다. 제안 모델의 핵심은 적어도 사이버 킬체인 공격 단계 중 원격 통신 채널을 형성하여 명령 및 제어 단계로 진입하기 이전에 위협을 식별하기 위한 구조이다. 이를 구현하기 위해서는 목표와 가설수립이 핵심 과제이자 대상을 명확히 하는 과정이다.

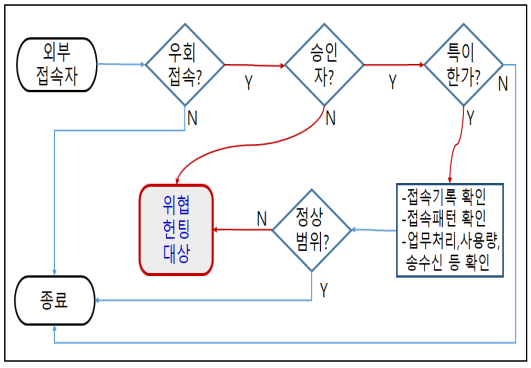

그림 3. 우회 원격 공격 위협 대상 식별
Fig. 3. Identifying of a circumvent remote attack threat target

1. 우회 원격 공격 대상 식별

첫 번째는 외부로부터 우회 원격 공격 위협의 대상을 식별하는 과정이고, 세부 진행 절차의 흐름도는 그림 3과 같다. 두 번째 과정은 이를 바탕으로 목표와 가설에 부합하는 내외부 위협 헌팅 절차를 수행한다. 또한, 이를 수행하는 과정은 〈알고리즘 1〉과 같다.

〈알고리즘 1〉 우회 원격 공격 대상 식별 알고리즘
단계 1 : /* 우회 접속자 유무 판단 */
외부에서 우회 접속자가 있는가?;
우회 접속자가 없으면 종료;
단계 2 : /* 승인된 우회 접속자 추출 */
승인된 접속자가 아니면 위협 헌팅 대상;
승인된 접속자로 특이사항 없음은 종료;
단계 3 : /* 승인된 특이 접속자 지표 확인 */
접속 시간, 패턴, 처리업무, 용량 확인;
송수신 시간, 용량 등 확인;
단계 4 : /* 지표 확인 결과 정상범위 판단 */
확인한 결과 정상 범위내이면 종료;
정상범위가 아니면 위협 헌팅 대상;

2. 위협 헌팅 수행 절차

두 번째로서, 위협 헌팅 수행 절차는 위협 헌팅 대상 선정 과정과 연계되어 분석 및 환류를 중심으로 4단계 절차로 구성된다. 첫 번째는 목표 및 가설, 두 번째는 정보수집, 세 번째는 수단 설정, 네 번째는 실행 및 검증 단계로 구분한다. 4단계의 절차는 기본적으로 순환하지만, 부분적으로 환류되어 반복하거나 전체 반복 수행으로 진행할 수도 있다. 그림 4는 조직적인 해킹그룹의 우회 원격 공격 위협에 대응하는 위협 헌팅 절차 모델이다.

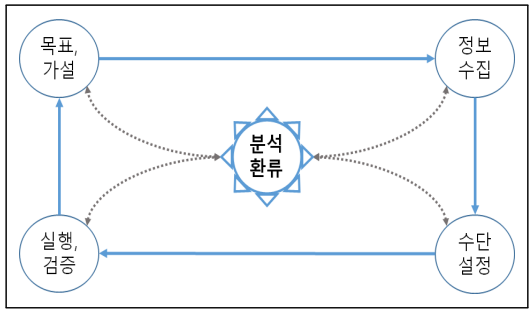

그림 4. 조직적 해킹 대응을 위한 위협 헌팅 절차
Fig. 4. Threat hunting process for organizational hacking response

가. 목표 및 가설

목표는 위협 헌팅 대상 체계와 수행 범위를 설정하여 위협을 찾고자 하는 명확한 범위와 예상하는 결과를 설정한다.

가설은 목표로 선정된 대상 체계에 위협이 존재한다는 가정을 전제로 한다. 주목해야 하는 주요 위협은 조직적인 해킹그룹이 수행하는 우회 원격 공격 위협이다. 그래서 위협의 존재를 가정한 가설은 적의 공격 목표, 탐지되지 않는 멀웨어 등 공격 도구와 공격의 전술, 기술 및 절차(TTPs)를 추정하는 것이다.

나. 정보수집

정보수집 단계에서는 조직적인 해킹그룹에 의한 우회

원격 공격 위협이 중요하므로 VPN 등 원격 접속자를 추출한 단서를 이용한다. 또한, 승인된 사용자와 침해시도자를 분류한 결과를 점검하고 수립된 가설을 기반으로 외부의 침해 사례 등 위협정보를 수집한다. 더불어 대상 체계에 대한 알려진 취약점, IoC(Indicator of Compromise, 침해지표) 및 TTPs 등을 수집하고 분류한다.[18] 정보수집은 가설을 기반으로 정제되고 효율성을 고려하여 수집되어야 한다. 수집된 정보는 수립된 가설을 논리적으로 뒷받침되고 분류 및 정제되어, 다음 단계인 수단 설정과 연계되어야 한다.

다. 수단 설정

가설을 증명하기 위해 어떤 도구와 자원을 사용할 것인지에 중점을 두고 접근하는 것이다. 이를 위해 갖추어야 할 요소는 헌터와 수단이다. 첫 번째는 헌터의 역량이 충분해야 하고, 헌터를 지원할 수 있는 시스템 관리자와 분석가 등 협력자가 필요하다. 더욱이 공격 유형별 전술과 기술 및 절차를 추정하고 분석할 수 있는 전문가의 지원도 필요하다. 두 번째는 헌터가 사용할 도구인 조사 및 분석 장비와 시각화 장비 등이 수반되어야 한다. 특히, VPN 등 우회 원격 공격의 원점 IP를 정확히 확인할 수 있는 도구가 준비되어야 한다. 접속자가 승인된 사용자만 있는 경우에도 원점 IP 확인을 위한 절차와 도구를 준비해야 한다. 이는 승인된 사용자가 도용이나 해킹을 당하여 악용될 수 있는 상황에 대비한 조치이다.

라. 실행 및 검증

실행에서는 가설에 기초한 수집된 정보와 자원 및 도구를 활용하여 위협 헌팅을 수행한다. 조직적인 해킹그룹의 우회 원격 공격에 주목하여 위협 흔적을 찾는 것이다. 여기서 위협 흔적은 해시값, IP 도메인, 네트워크 및 호스트 정보 등 침해지표와 해커가 사용한 도구뿐만 아니라 TTPs 등을 말한다.

검증은 수집된 정보와 위협 헌팅 실행 결과로 도출된 자료들을 활용하여 수립된 가설을 증명하는 과정이다. 특히, 우회 원격 공격 위협 흔적이나 대상 체계에서 도출된 침해지표와 TTPs를 유추하여 가설 검증과 특이사항을 추출한다. 실행 및 검증은 결과에 무관하게 실행환경과 사용된 도구들을 분류하여 정리한다. 위협 흔적을 발견한 때에는 식별된 위협을 찾아서 제거하거나 정보보호 체계에 차단 및 탐지 정책으로 설정하여 방어 조치를 보강한다.

위협의 실체나 흔적을 발견하지 못한 경우에는 가설수립, 정보수집 및 수단 설정에서 부족한 부분을 보충하고 보완사항을 조정한다. 또한, 수행 과정에서 수집되고 산출된 자료는 목표 및 가설수립 단계로 연계되고 분석 및 환류 기능에 전달된다.

마. 분석 및 환류

여기에서는 위협 헌팅 과정의 전체 절차 중에서 지속적인 분석과 환류의 핵심적인 기능을 수행한다. 이 기능의 역할은 헌터가 수행하는 단계별 각종 자료를 분석해야 한다. 또한, 종합되고 분석된 자료는 적절한 단계에 제공되어 헌팅 수행을 촉진하는 역할을 해야 한다.

첫 번째로 목표 및 가설 수립단계에서는 수립된 목표와 가설에 대해 외부 원격 공격 위협에 대응한 가설 설정의 적정성을 검토하여 결과를 피드백한다. 두 번째로 정보수집 단계에서 수집된 자료가 정확성, 충분성, 영향성을 검토하여 피드백하거나 보충 자료를 제공한다. 특히, 우회 원격 접속자 수집자료와 위협 헌팅 대상 체계에서 식별된 침해지표 및 TTPs 등의 자료를 분석하여 제공한다. 세 번째는 실행 및 검증 결과로 식별된 새로운 멀웨어 등 흔적이나 TTPs 도출을 위해 상관관계 등 다양한 관점에서 분석한다. 특별히 원격 우회 접속자 자료와 식별된 위협 흔적들 사이의 연관성을 중점적으로 분석한다. 네 번째는 실행되어 검증된 가설과 정보 및 수단들의 변경이나 증감할 요소는 없는지 분석한다. 다섯 번째는 종합적 분석 자료를 반복 수행과 방어정책 수립 등으로 환류하여 후속 조치로 보완한다.

Ⅳ. 실험 및 결과

제안한 방법을 검증하기 위해 국방 인터넷 서비스 환경에서 실험하였다. 이를 위한 수행 과정을 그림 5의 크게 두 가지 과정과 같은 흐름으로 실험하였다.

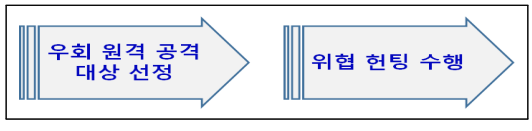

그림 5. 우회 원격 공격 위협탐지를 위한 위협 헌팅 절차
Fig. 5. Threat hunting procedure for circumvent remote attack threat detection

실험 환경으로, VPN을 사용한 공격자가 국방 인터넷 서비스망에서 운영 중인 웹서버를 대상으로 악성 행위를

수행하고, 위협 헌터는 원점 IP 확인 방법 활용과 시스템 로그 확인을 통해 공격자의 행위를 파악하였다.

구체적인 실험 환경은 아래 그림 6과 같다. 웹서버는 리눅스 운영체제이고 아파치2로 구축되었으며 IP 정보는 보안상 비공개로 한다. 공격자는 윈도우10 PC를 사용하였고 기존 IP는 223.38.94.190이지만, 공격자가 VPN을 사용하였기 때문에 웹서버에서는 VPN External IP인 11.140.2.36으로 인식한다.

그림 6. 국방 인터넷 서비스에서 시험환경 구성
Fig. 6. Test environment configuration in defense internet service

1. 우회 접속자 판단

공격자가 웹서버에 접속하면 그림 7과 같이 원점 IP 확인 스크립트가 실행되고 웹서버에서는 공격자의 접속 IP와 원점 IP를 비교하여 VPN을 사용한 우회 접속자 여부를 확인할 수 있다. 아래 그림 8은 우회 접속자 확인 화면이다.

그림 7. 원점 IP 확인을 위한 스크립트 실행 화면
Fig. 7. Script execution screen to check origin IP

접속 IP	원점 IP
11.140.2.36 11.140.2.36	Origin_IP=223.38.94.190 Origin_IP=223.38.94.190

그림 8. 우회 접속자의 접속 IP와 원점 IP
Fig. 8. Connection IP and origin IP of circumvent accessor

2. 가설 생성

위협 헌터는 우회 접속자에 대한 정보보호체계 탐지 및 차단 로그를 확인하였다. 공격자 IP의 접근기록에 대한 통계를 확인한 결과는 표 1과 같이 나타났다.

표 1. 공격자 IP의 최근 24시간 동안의 접근기록
Table 1. Access history of the attacker's IP for the last 24 hours

목적지 포트	접근 횟수
443	16,366
80	3,873
23	30
22	21
21	15

공격자는 최근 과도한 웹 페이지 접속 및 원격 접속 시도였음을 알 수 있다. 이는 웹 응용체계 및 서버의 취약점을 탐색한 정찰 행위로 추정할 수 있다. 그리고 공격자가 성공하였다면 주요 정보 유출, 시스템 파괴 등의 다양한 악성 행위가 가능하다. 따라서 위협 헌터는 공격자가 웹서버에 접속하여 주요 파일의 유출을 시도한다는 가설을 생성한다.

3. 정보수집

위협 헌터는 생성한 가설에 따라 외부 사이버 위협 정보와 내부 자산에 대한 위협 상황을 파악하였다. 이 정보들을 근거로 필요한 도구를 선정하고 가설 검증으로 연결할 수 있다. 먼저, 최근 보안뉴스 기사에 따르면 웹 사이트의 개인 정보가 유출되어 다크웹 상에서 거래되는 사례가 빈번히 발생하고 있다는 외부 사이버위협 정보를 확인하였다. 이는 최근 2년간 지속적으로 발생하고 있는 현상으로, 웹서버 운영자 관점에서 주의해야 할 위협이다. 또한 표 1에서 확인한 것과 같이 내부 웹서버에 대한 원격 접속 시도가 지속되기 때문에 이에 대한 분석이 필요하다.

4. 도구 선정

외부 일반 인터넷 영역과 국방 인터넷 영역의 가장 큰 차이점은 서버를 보호하는 다중 정보보호체계의 유무일 것이다. 정보보호체계 로그를 통해 공격자의 공격 행위를 추적할 수 있다면 위협 헌팅 효과를 향상할 수 있다. 이번 위협 헌팅에서는 방화벽, IPS, 통합보안관제체계의 로그를 중심으로 위협 헌팅을 수행하였다. 또한 서버의 시스템 명령어를 확인 및 저장할 수 있는 Putty등의 도구를 추가로 사용하였다.

5. 가설 검증

먼저 위협 헌터는 방화벽 및 IPS의 세부 로그를 확인

하였다. 표 2의 로그를 통해 공격자의 활동 시간과 접근 파일 등의 침해지표를 확인할 수 있었다.

표 2. 정보보호체계에서 탐지된 공격자 IP의 로그
Table 2. Log of the attacker's IP detected in the information protection system

날짜	시각	방호체계	로그기록	비고
3. 17.	17:13:13	방화벽	차단	22포트
3. 17.	17:13:51	방화벽	차단	22포트
3. 17.	17:15:42	방화벽	차단	22포트
3. 17.	17:16:20	방화벽	차단	22포트
3. 17.	20:05:10	IPS	차단	/etc/passwd

위 표 2와 같이 공격자는 22번 포트로 지속적인 원격 접속을 시도하여 주요 정보인 /etc/passwd 파일에 접근 및 유출을 도모하였다. 위협 헌터는 로그 분석으로 서버 내부 침해지표를 세부적으로 확인하였다.

이어서 서버 관리자 계정의 로그인 기록을 lastlog 명령어를 통해 마지막 로그인 기록을 확인할 수 있다. 그림 9와 같이 공격자가 17:30부터 수차례 서버에 접속하였음을 확인할 수 있다. 방화벽에서 접근이 차단되어 이를 우회할 수 있는 경로를 통해 접속한 것으로 추정된다.

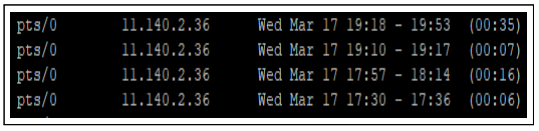

그림 9. lastlog 명령어의 수행 결과
Fig. 9. Execution result of lastlog command

위협 헌터는 수집한 정보를 바탕으로 가설을 검증하기 위해 정보보호체계 로그에서 확인한 /etc /passwd 파일에 대한 접근기록을 확인한다. touch 명령어를 통해 해당 파일에 대한 생성, 변경 및 접근 시간을 확인하였다. 그림 10은 /etc/passwd 파일에 대한 touch 명령어 수행 결과이다.

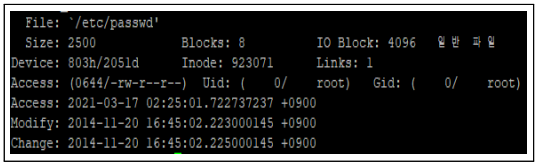

그림 10. touch /etc/passwd 명령어의 수행 결과
Fig. 10. Result of executing the touch /etc/passwd command

로그 확인 결과, 공격자는 3월 17일에 /etc/passwd 파일에 접근하였음을 알 수 있다. 해당 파일을 복사하여 외부로 유출을 시도했을 가능성이 가장 높다. 시간이 02:25로 공격자의 접속보다 이전 시간으로 되어있는 것은 분석에 혼선을 주기 위해 공격자가 시간 정보를 변경한 것으로 추정할 수 있다.

6. 결과 분석 및 환류

최종적으로 위협 헌터는 정보보호체계와 서버에서 확인한 침해지표를 통해 실제로 공격자가 웹서버에 접속하여 주요 파일에 접근한 기록을 확인할 수 있었다. 이에 대한 조치로 서버 비밀번호 변경 및 접근 정책을 정리하고, DB 암호화를 통해 주요 정보에 대한 접근을 차단하였다. 또한 위협 헌팅 과정에서 산출된 자료는 차후 분석과 위협 헌팅에 활용하기 위해 저장하였다.

V. 결론 및 향후 과제

본 논문에서는 조직적인 해킹그룹의 표적형 우회 원격 공격 위협탐지를 위한 위협 헌팅 모델을 제안하였다. 방어 관점에서 제안한 모델은 사이버 킬체인 단계 중 최소한 명령 및 제어 단계 이전에서 대응하여 성공적인 방어를 보장하는 효율적인 방안이다. 또한, 위협 헌팅 대상과 목표 선정을 명확히 하여 효율성과 적시성을 향상할 수 있는 유용한 모델이다.

제안한 모델은 실제 국방 환경에서 실험하여 실효성을 검증하였다. 특히, 위협 헌팅 수행 절차에서 수집한 정보를 통한 공격 절차 유추는 전체 절차 중에서 핵심적인 기능으로 분석 능력 등 헌터의 전문화된 능력이 필수적인 요소로 확인되었다. 그리고 제안한 방법은 조직적인 해킹그룹의 사이버 위협에 대응하는 하나의 접근방법이다. 이를 기반으로 기관이나 기업의 정보체계 구성 환경의 특성을 고려한 적용으로 새로운 통찰과 성과로 이어지길 기대한다.

향후 과제로, 첫 번째는 우회 원격 공격자에 대한 역추적 방법이다. 두 번째는 조직적인 해킹그룹의 정체를 식별하는 방법 연구가 필요하다. 세 번째는 IoC와 TTPs 등을 추적하고 축적하여 다양한 변화에 신속히 대응할 수 있는 방어체계 구축방안이 연구되어야 할 것이다.

References

[1] M.Zain ul Abideen, S. Saleem, and M. Ejaz, "VPN Traffic Detection in SSL-Protected Channel", Security Communication Networks, pp. 1-17, Oct. 2019. DOI: https://doi.org/10.1155/2019/7924690

[2] R. Angelo, "Secure Protocols and Virtual Private Networks: An Evaluation", Issues in Information Systems vol. 20, Issue 3. pp. 37-46, 2019. DOI:https://doi.org/10.48009/3_iis_2019_37-46

[3] Yogesh Kumar Sharma, Chamandeep Kaur, "The Vital Role of Virtual Private Network(VPN) in Making Secure Connection Over Internet World", International Journal of Recent Technology and Engineering(IJRTE) vol. 8 Issue-6, pp.2336-2339, March 2020. DOI:10.35940/ijrte.F8335.038620

[4] Zhang Zhipeng, Sonali Chandel, Sun Jingyao, Yan Shilin, Yu Yunnan, Zang Jingji, "VPN: aBoon or Trap?:A Comparative Study of MLPS, IPSec and SSL Virtual Private Networks", Second International Conference on Computing Methodologies and Communication(ICCMC), pp. 510-515, IEEE, Feb. 2018, Erode, India DOI:10.1109/ICCMC.2018.8487653

[5] Scott Pellyi, "FBI Director on Threat of ISIS, Cybercrime", CBS News, Oct. 5. 2014, DOI:www.cbsnews.com/news/fbi-director-james-comy-on-isis-cybercrime/

[6] Symantec, "Internet Security Threat Report", Vol. 22, Apr. 2017. DOI: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[7] Yoon-Cheol Hwang, Hyung-Jin Mun, "Intrusion situation classification Model for Intelligent Intrusion Awareness", Journal of Convergence for information Technology Vol. 9. No. 3, pp. 134-139, 2019. DOI: https://doi.org/10.22156/CS4SMB.2019.9.3.134

[8] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1.1, 80, 2011. DOI:https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[9] Sqrrl Inc., "A framework for Cyber Threat Hunting", 2016. DOI: https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper-web.pdf

[10] Dan Gunter, Mac Seitz, "A Practical Model for Conducting Cyber Threat Hunting", SANS, Mar. 2019. https://www.sans.org/white-papers/38710/

[11] David J Blanco, "The Pyramid of Pain", Mar. 2013. DOI: http://detect-respond.blogspot.com/2013/the-pyramid-of-pain.html

[12] MITRE, "ATT&CK MATRIX for Enterprise", DOI: https://attack.mitre.org/

[13] Inhwan Kim, Dukyun Kim, Sungkuk Cho, Byungkook Jeon, "A Method for Original IP Detection of VPN Accessor", The Journal of The Institute of Internet, Broadcasting and Communication(IIBC) Vol. 21, No. 3, pp.91-98, Jun. 30, 2021. DOI:https://doi.org/10.7236/JIIBC.2021.21.3.91

[14] Fireeye Mandiant, "M-trends 2020 report", DOI:http://www.fireeye.com/m-trends/rpt-m-trends-2020

[15] R. Stillions, "The DML Model", 22 Apr. 2014. DOI:http://ryanstillions.blogspot.com/2014/the-dml-model_21.html

[16] S. Bromander, A. Jøsang, M. Eian, "Semantic Cyberthreat Modelling", STIDS Proceedings, pp. 74-78, 2016. DOI:https://stids.c4i.gmu.edu/papers/STIDSPapers/STIDS2016_A2_BromanderJosangEian.pdf

[17] Hochan Ryu, Kyeongmin Jo, Inhwan Kim, "A study on the application of threat hunting to the defense information system",Journal of Defense and Security Vol. 2. No. 2. pp. 59-81, Dec. 2020. DOI:https://www.dssc.mil.kr/dssckr/174/subview.do

[18] Hyeisun Cho, Seulgi Lee, Nakhyun Kim, Byungik Kim, Dongyoung Yoo, Moon-hyun Kim, "Analysis of Cyber Threat Level based on Indicator of Compromise", korea information processing society spring conference Vol. 24, No. 1, page 291-294, Apr. 2017. DOI:https://doi.org/10.3745/PKIPS.Y2017M04A.291

[19] I. Jeon, S. Kang, H. Yang, "Development of Security Quality Evaluate Basis and Measurement of Intrusion Prevention System," Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 11, No. 1, pp. 81-86, 2010. DOI:https://doi.org/10.5762/KAIS.2010.11.4.1449

저 자 소 개

김 인 환(정회원)

- 1989년 : 금오공대 전자공학(공학사)
- 1997년 : 일본 게이오대 전기공학(이공학석사)
- 2018 ~ 현재 : 강릉원주대 박사과정
- 주관심분야 : 사이버 보안, 모바일 S/W, 에이전트 S/W
- E-mail : casasagi@naver.com

류 호 찬(비회원)

- 2016년 : 고려대학교 사이버국방학과 (공학사)
- 2017 ~ 현재 : 고려대학교 정보보호대학원 석사과정 재학
- 2016 ~ 현재 : 육군 장교 재직
- 주관심분야 : IDC보안, 생체인증, AI 보안
- E-Mail : ryuhochan@korea.ac.kr

조 경 민(비회원)

- 2017년 : 고려대학교 사이버국방학과 (공학사)
- 2018 ~ 현재 : 고려대학교 정보보호대학원 석박사통합과정 재학
- 2017 ~ 현재 : 육군 장교 재직
- 주관심분야 : IoT, Smart Home, Network Security
- E-Mail : elision@korea.ac.kr

전 병 국(정회원)

- 1985년 : 광운대 전산과(이학사)
- 1991년 : 광운대 대학원 컴퓨터과학과 (이학석사)
- 2000년 : 광운대 대학원 컴퓨터과학과 (이학박사)
- 1991 ~ 1993년 : KISTI 연구원
- 1993 ~ 현재 :강릉원주대 교수
- 주관심분야 : 커넥티드 카, 자율주행차, IoT, 모바일 에이전트 S/W
- E-Mail : jeonbk@gwnu.ac.kr