https://doi.org/10.33778/kcsa.2022.22.1.019

사이버 거점을 활용한 위협탐지모델 연구★

김 인 환*, 강 지 원**, 안 훈 상***, 전 병 국****

요 약

ICT 기술의 혁신적인 발전에 따라 해커의 해킹 수법도 정교하고 지능적인 해킹기법으로 진화하고 있다. 이러한 사이버 위협에 대응하기 위한 위협탐지 연구는 주로 해킹 피해 조사분석을 통해 수동적인 방법으로 진행되었으나, 최근에는 사이버 위협정보 수집과 분석의 중요성이 높아지고 있다. 봇 형태의 자동화 프로그램은 위협정보를 수집하거나 위협을 탐지하기 위해 홈페이지를 방문하여 악성코드를 추출하는 다소 능동적인 방법이다. 그러나 이러한 방법도 이미 악성코드가 유포되어 해킹 피해를 받고 있거나, 해킹을 당한 이후에 식별하는 방법이기 때문에 해킹 피해를 예방할 수 없는 한계점이 있다. 따라서, 이러한 한계점을 극복하기 위해 사이버 거점을 식별, 관리하면서 위협정보를 획득 및 분석하여 실질적인 위협을 탐지하는 모델을 제안한다. 이 모델은 방화벽 등의 경계선 외부에서 위협정보를 수집하거나 위협을 탐지하는 적극적이고 능동적인 방법이다. 사이버 거점을 활용하여 위협을 탐지하는 모델을 설계하고 국방 환경에서 유효성을 검증하였다.

A Study on Threat Detection Model using Cyber Strongholds

Inhwan Kim*, Jiwon Kang**, Hoonsang An***, Byungkook Jeon****

ABSTRACT

With the innovative development of ICT technology, hacking techniques of hackers are also evolving into sophisticated and intelligent hacking techniques. Threat detection research to counter these cyber threats was mainly conducted in a passive way through hacking damage investigation and analysis, but recently, the importance of cyber threat information collection and analysis is increasing. A bot-type automation program is a rather active method of extracting malicious code by visiting a website to collect threat information or detect threats. However, this method also has a limitation in that it cannot prevent hacking damage because it is a method to identify hacking damage because malicious code has already been distributed or after being hacked. Therefore, to overcome these limitations, we propose a model that detects actual threats by acquiring and analyzing threat information while identifying and managing cyber bases. This model is an active and proactive method of collecting threat information or detecting threats outside the boundary such as a firewall. We designed a model for detecting threats using cyber strongholds and validated them in the defense environment.

Key words : Cyber Strongholds, Cyber Threat Intelligence, Threat Detection, Advanced Persistent Threat

접수일(2021년 12월 3일), 수정일(2021년 12월 23일), 게재확정일(2021년 12월 31일)

★ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었음. (No, UD210029TD)

* 세종대학교/컴퓨터공학과(주저자)

** 세종대학교/컴퓨터공학과(공동저자)

*** 강릉원주대학교/소프트웨어학과(공동저자)

**** 강릉원주대학교/소프트웨어학과(교신저자)

1. 서론

적대적 해킹그룹의 공격 위협에 대비하기 위한 최선의 방안은 적대적 해킹그룹의 활동을 24시간 365일 감시정찰하여 그들의 의도와 활동을 예측하고 선제적으로 대책을 강구 할 수 있는 능력과 태세를 갖추는 것이다. 선제적 대책 강구는 적대적 해킹그룹에 비용과 고통을 유발하게 함으로써 공격 위협의 실제 실행을 지연시키거나 실행 즉시 탐지되어 그들의 목표 달성을 좌절시킬 수 있는 것이다.

해커의 기술은 방어 시스템보다 앞서 나가고, 방어 체계를 뚫을 새로운 방법을 찾기 위해 노력하고 있으므로 예방이 가장 중요하다. 이를 위한 방법은 조직의 사이버 위협에 대한 정보를 이해하고 평가한 다음, 해당 지식을 지속적인 방어 능력 향상에 적용하는 것이 하나의 접근방법이다. 이것은 국가안보 분야의 전통적인 전력 중에서 정보감시정찰(ISR, Intelligence Surveillance Reconnaissance)과 같은 기능을 하는 것이다. 이러한 맥락에서 사이버 위협정보(CTI, Cyber Threat Intelligence)에 관한 기술적인 분야의 연구는 크게 2가지 분야로 발전되어 왔다[1-3]. 하나는 사이버 위협정보 공유, 표준화 방법, 분류, 프레임워크 등으로 이루어져 왔으며[4, 5], 다른 한 분야는 사이버 위협정보를 해킹 피해 사건 조사분석을 통해 추출한 악성코드, 악성코드 경유지, 악성코드 유포 사이트 등을 정보보호체계에 반영, 차단하는 것으로 발전되어 왔다[6, 7].

다소 적극적인 위협정보 탐지 방법으로는 봇(bot) 형태의 프로그램에 의한 인터넷 홈페이지를 자동으로 방문하여 웹 크롤러를 사용한 악성코드를 추출하는 방법도 상용화되었다[8]. 그러나 이러한 방법도 이미 악성코드가 유포되어 해킹 피해를 받고 있거나, 피해를 받은 이후에 식별하는 방법이기 때문에 해킹 피해를 예방할 수 없는 한계점이 있다.

따라서, 이러한 한계점을 극복하기 위해 사이버 거점을 식별, 관리하면서 위협정보를 획득 및 분석하여 위협을 예측하거나 탐지하는 접근방법이 필요하다.

본 논문에서는 사이버 거점[1]을 활용하여 위협탐지 모델을 제안한다. 이 모델은 방화벽 등의 경계선 외부에서 위협정보를 수집하거나 위협을 탐지하는 것이다. 따라서, 경계선 외부에서 위협을 탐지하는 적극적인 위협탐지 모델을 설계하고 검증한다.

본 논문의 구성으로 2장에서는 사이버 위협정보 수집과 탐지에 관한 기존 연구에 대해 알아본다. 3장에서는 사이버 거점을 활용하여 위협을 탐지하는 모델을 제안한다. 4장에서는 실험을 통해 제안한 위협탐지 방법의 유효성을 검증하였다. 마지막으로 결론 및 향후 연구 방향을 논한다.

2. 선행 연구

2.1 사이버 위협정보 및 생산

사이버 위협정보란 수집된 사이버 위협 첩보를 분석 및 평가되고 해석된 것을 의미한다. 파이어아이에서는 사이버 위협정보를 생성하는 과정을 5단계로 구분하여 CTI 프로세스 라이프사이클이라고 한다[9]. 가트너는 현존하거나 발생 가능한 위협에 대한 대응을 결정하기 위해 해당 위협에 대한 맥락(context), 메커니즘, 지표, 예상 결과 및 실행 가능한 조언 등을 포함하는 증거기반의 지식으로 정의하고 있다[10].

이러한 CTI는 금융, 공공, IT 등 다양한 분야에 종사하는 사이버보안 담당자 80.8%가 효과가 있다고 응답한 자료를 SANS의 2019 CTI 보고서에서 발표하였다[11]. 이에 따라 KyeongHan Kim 등은 OSINT(Open Source Intelligence) 기반의 활용 가능한 사이버 위협정보 수집 및 연관관계 표현 시스템을 소개하였다[12].

2.2 사이버 위협탐지를 위한 인지 기술

사이버 위협으로부터 방어하기 위해서는 조직의 자산을 보호하는 경계선에서 위협을 탐지 및 차단하여야 한다. 이를 위한 첫 번째가 위협을 인지하는 과정이다. 두 번째가 정보보호체계에서

1) 사이버 거점은 해킹그룹의 APT 공격 과정에서 명령 및 통제(C2) 서버와 탈취한 자료를 임시로 보관하는 수집 서버 등을 점령한 상태로 활동하는 사이트를 통칭하는 용어로 사용한다.

※ 이와 별도로 은닉 사이트는 악성코드를 숨겨 놓거나 퍼뜨리는 목적으로 경유지 및 유포지라는 용어로 사용.

탐지하는 것이며, 세 번째가 탐지됨과 동시에 차단되어 내부로 침투를 막는 것이다. 이와 관련된 연구로, 보안 이벤트 시각화 기술 조사와 신종 공격기법 및 분석 기술의 현황을 분석하였다[13]. 그리고 APT 공격 탐지에 적합한 공격 경로 및 의도 분석 시스템의 구조를 제안하였다[14]. 또한, 조직의 경계선에 설치된 정보보호체계에서 발생한 위협 이벤트를 수집하여 통계 기반의 상관관계 분석과 위협경보 간 상호 인과관계를 학습하는 모델을 구축하여 기계학습 기반의 공격 경로 재구성 및 위협 예측 기술을 제안하였다[15]. 이와 같은 기법들은 위협탐지를 위한 인지 능력 향상을 위한 방법들이라고 할 수 있다.

2.3 사이버 위협탐지 기술

사이버 위협에 대한 방어는 위협을 탐지하여 차단하거나 침해 시도를 거부하는 것이다. 이와 관련된 연구는 주로 경계선에 설치된 정보보호체계의 기능과 성능을 보강하는 방법과 침해사고 조사 및 분석 과정에서 위협의 실체인 백도어 등의 악성코드를 식별하여 해시값, 시그니처, IP나 URL 등의 침해지표를 정보보호체계에 반영하는 방법으로 진행되어왔다. 위협정보 탐지 대응 시간을 모델링하였고[16], 탐지와 대응 효율성을 향상하는 보안체계 조합형 보안 서비스 모델 등이 연구되었다[17]. 침해사고 탐지 방법을 정의하고, 성능테스트를 통해 효율적인 보안 관제를 위한 방안을 제시하였고[18], VPN 접속자의 원점 IP를 탐지하는 방법을 제시하였다[19]. 또한, 모자이크 전 수행개념을 적용한 능동형 상황 탄력적 사이버 방어작전을 제안했다[26]. 이러한 연구들은 위협을 탐지하거나 탐지된 위협에 대한 대응 효율성을 향상하는 수세적, 수동적 방법들이다.

이에 반해, 능동적 방법은 적대적 해킹그룹이 구축한 사이버 거점을 정찰하여 그들의 목적, 해킹 기술 수준, 주요 표적, 전술, 무기 등의 위협정보를 탐지할 수 있다. 따라서 본 논문에서는 사이버 거점을 활용한 위협탐지 모델을 제안한다.

3. 사이버 거점을 활용한 위협탐지 모델

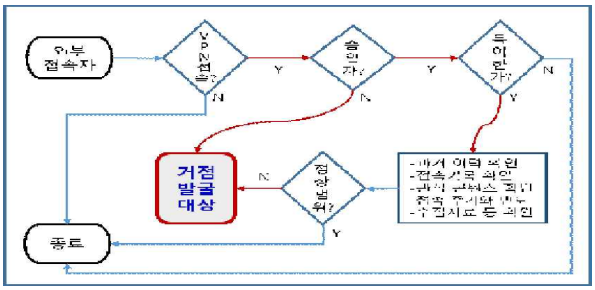
사이버 거점을 이용한 해킹 유형은 3가지가 있을 수 있다. 첫 번째는 조직적인 해킹그룹에서 해커가 구축한 C&C 서버에 백도어를 설치한 경우이다. 두 번째는 피해 웹사이트를 공유하는 것이다. 세 번째는 특정한 지역이나 산업에 특화된 해커를 공격하여 해당 해커가 구축해 놓은 인프라들을 착취하고 특정한 사람을 목표로 한다.

일반적으로 이러한 사이버 거점은 통신품질의 신뢰성, 이용의 편의성, 탐지나 회피 용이성, 장비성능 등의 가용성 및 방어력이 허술하거나 관심에서 자유로운 지점 등을 고려하여 구축한다.

3.1 사이버 거점 발굴

적대적 해킹그룹의 공격 위협을 감시정찰하기 위해서는 먼저 사이버 거점을 발굴해야 한다. 이를 위한 쉬운 수동적 방법은 2가지가 있다. 첫 번째는 해킹 피해 사건을 조사분석 과정에서 식별하는 방법이고, 두 번째는 사이버보안 협력관계의 국내외 기관이나 보안기업으로부터 협조를 받아서 관리하는 방법이 있을 수 있다. 이에 반해, 능동적 방법은 사이버 거점을 적극적으로 찾아서 발굴하는 것이다.

그러면 능동적 방법인 사이버 거점을 어떻게 적극적으로 찾을 수 있느냐의 문제이다. 이것은 적대적인 해킹그룹에서 APT 공격을 위해 대부분의 활동 과정에서 이용하는 VPN 우회 접속 방법을 역으로 이용하는 것이다. 우선 VPN 접속자인지를 확인하는 방법은 VPN 접속자의 원점 IP 탐지 방법을 활용하는 것이다[19]. 이 방법에서 개발한 알고리즘을 이용하면 VPN IP와 원점 IP를 모두 알 수 있으므로 VPN 접속자를 확인할 수 있다. 이외에도 VPN 서비스 사이트의 주소를 제공하는 제품을 이용하거나 Shodan 등의 도구들을 이용하여 수동으로 구별해 내는 방법도 있다. 적대적 해킹그룹에서 정찰 활동이나 정보수집을 위한 홈페이지 방문자 중에서 VPN 우회 접속자를 추출하여 거점(원점)을 찾는 범위를 한정하여 발굴하는 것이다. 아래 그림은 간략한 절차의 흐름을 나타내는 구성도이다.



(그림 1) 사이버 거점 발굴 대상추출 절차도

알고리즘 1은 사이버 거점 발굴하기 위해 대상을 추출하는 과정을 나타내고 있다.

<알고리즘 1> 거점발굴 대상추출 알고리즘

```
begin
 /* check VPN circumvent connection */
    try to connect to the Web server by
                        unknown users;
    if access method != VPN then exit;
 /* check user authentication */
    else if the approved users == No then
      set as cyber strongholds excavation targets;
 /* check user behavior range */
    else if user behavior range == NORMAL
       then exit;
 /* whether or not inbound the check lists */
    else set as excavation targets;
 /* extracts list of excavation targets */
    get list of excavation targets;
end
```

대부분의 사이버 거점 발굴은 수동적인 방법과 능동적인 방법 및 협력체계 등 가용한 모든 방법을 활용하는 것으로 볼 수 있다.

3.2 사이버 거점 관리

사이버 거점에서 탐지하는 위협정보는 공격에 사용되는 무기인 각종 도구이다. 이를 통해 무기의 정교함 등 기술 수준과 어느 국적의 어떤 해킹그룹에서 제작한 것인지 등 특성을 가늠할 수 있고, 무기들의 기능을 분류하여 전술적 특성도 유추할 수 있다. 또한 이러한 무기들을 분석하여 방어체계에 선제적으로 반영하여 적대적 해킹그룹의 노력을 무위로 돌릴 수 있다. 이와 같은 상황에서 적대적 해킹그룹은 공격 목적을 달성하기 위하여 노출된 무기를 대체하는 무기 개발 또는 새로운 전술을 수립하는 등의 추가적인 준비시간과 소요 비용 증가를 초래한다. 또한, 사이버 거점에서 적대적 해킹그룹이 탈취한 자료를 저장해 둔 것을 획득한다면 이들이 노리는 것이 무엇인지 대략 유추할 수 있다.

따라서 사이버 거점을 관리하기 위한 기본적인 항목은 IP, URL 등 어디에 있는 것인지가 파악되어야 하고, 접속할 수 있는 계정과 패스워드는 필요한 것인지 그리고 필요한 것이면 무엇인지가 명확해야 한다. 그리고 거점의 상태 등이 포함되어야 한다. 구체적인 항목은 표 1과 같이 구성할 수 있고, 추가나 구체화 관리할 수 있다.

<표 1> 사이버 거점 관리 항목

구분	주 항목	보조 항목
접속정보	IP, URL	브라우저, FTP 등
계정정보	계정명	패스워드
점검정보	설치파일 정상 유무 등	변형 여부 확인
주의사항	새로운 도구 설치 여부	삭제나 접근금지
거점상태	정상 또는 일시 불가 등	폐쇄 또는 이전 등
기타	확인 주기 등	

3.3 사이버 거점 정찰

일반적으로 사이버보안 연구자들은 공격자의 패턴과 무기를 식별하여 공격의 목표를 찾아내고 공격자 행동을 구별하는 노력을 지속한다. 그러나 해커들이 다른 공격자를 해킹한 뒤 똑같은 무기를 사용하고 똑같은 피해자를 해킹하면서 공격 목표를 찾는 것과 공격자 구별이 어렵게 되었다. 이는 주로 조직적인 해킹그룹에서 외국 조직을 공격하는 해커들이 이런 유형의 전술과 기술을 모방하고 있다고 추정한다. 이러한 이유로 기관이나 기업의 사이버 방어조직과 보안 연구자들은 이와 같은 공격을 탐지할 수 있으며, 위협정보 맥락에서 해석할 수 있어야 할 것이다.

이와 같은 해커를 해킹하여 정보를 수집하는 정찰 방법에는 2가지 접근법이 있다. 첫 번째는 해커의 정보를 피해 장비로부터 수집 또는 명령/제어 서버로 전송되는 중간에 가로채는 간접 정찰 방법이다. 이러한 해킹 공격은 쉽지 않지만 탐지하는 것이 불가능하여 노출될 위험이 극히 낮은 장점이 있다. 반면, 두 번째 접근법은 다른

해커가 구축해 놓은 거점에 침투하는 직접 정찰 방법이다. 이럴 경우, 해커를 해킹하는 공격자는 탐지될 위험을 어느 정도 감수해야 하지만, 이로 인한 손실보다 획득할 수 있는 이익이 훨씬 크다고 예상되는 때에 활용하는 방법이다.

3.4 위협정보 획득 및 대응

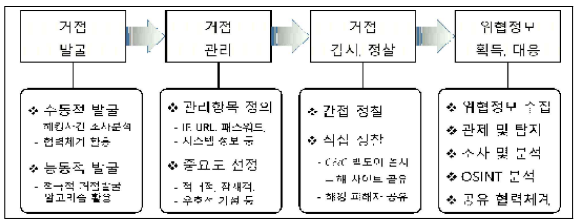
거점으로부터 획득한 위협정보는 국가 기관이나 기업이 과거, 현재 및 미래의 위협을 더 잘 이해하기 위한 자료를 의미한다. 수집된 위협정보는 조직의 네트워크 운영에 대한 상태 정보를 제공하며, 잠재적인 위협을 식별하고 향후 공격으로부터 보호하는 데 도움이 된다[20, 21]. 그래서, 정부 기관과 기업들은 기밀자료, 민감하거나 중요한 자료를 보호하고 향후 공격으로부터 피해를 예방하기 위해서는 공격자의 다음 단계 의도와 행동을 예측하고 이해해야 한다.

공격자들의 주요 위협은 악성코드, 웹 기반 공격, 웹 애플리케이션 공격, 서비스 거부, 봇넷, 피싱, 스팸, 랜섬웨어, 내부자 위협, 물리적 조작/손상/도난/분실, 익스플로잇킷, 데이터 침해, 신원 도용, 정보 유출, 취약점 등이다[22]. 이러한 조직적인 해킹그룹을 포함한 공격자들의 위협에 대비하기 위해 아래 5가지의 위협탐지 및 대응을 이해, 분석 및 발전시키는 것이 중요하다[12, 23].

① 사이버 위협정보 수집 : 사이버 거점을 발굴, 관리 및 감시정찰로 위협정보를 수집한다.
② 시스템 관제 및 탐지 기술 : 지속적이고 포괄적인 네트워크 및 엔드포인트(Endpoint)[2]의 감시이며, 호스트에 대한 전체 패킷 캡처 및 행위 기반 위협탐지 기능이 포함되어야 한다.
③ 고급 조사 및 분석 기술 : 이상 징후가 탐지되면 조사를 가속화 할 수 있는 고급 분석 기술 인력이 투입되어야 하며, 네트워크 트래픽과 같은 대량의 정보를 거의 실시간으로 검색하여 이상 징후를 탐지한다. 그리고 악성코드를 분석하여 실제 행위를 알아내고 적대적 활동의 한계와 범위를 식별해 내는 것이다.
④ OSINT 분석 및 생산 능력 : 정보 상황 맥락에서 사용할 공개 도구 또는 출처로부터 수집한 정치, 경제, 외교, 사회, 문화, 의료, 환경 등 모든 분야의 관계나 연관성을 이해하고 분석한다. OSINT는 6가지[3]로 분류할 수 있다.
⑤ 위협정보 공유체계 구축 : 국내외 기관 및 보안기업 등과 위협정보 공유체계를 구축한다.

위와 같이 위협정보를 획득하여 악성코드 등 구체적인 위협을 탐지해 내는 것이다. 또한, 위협정보는 사이버 거점으로부터 획득하기도 하지만, 타 정보와 융합하여 위협의 실체를 더욱 선명하게 할 수도 있고, 공격 위협의 실행 시기 예측에도 도움이 될 수 있다.

따라서, 해킹으로부터 방어하기 위해 5가지의 위협탐지 및 대응 방법을 최신화하면서 감시정찰로 적대적 해킹그룹의 활동과 의도를 파악하여 정보보호체계에 반영하는 등의 활동이 위협탐지에 무엇보다 중요하다. 이러한 방어 활동에서 위협탐지 활동 체계를 도식화하면 그림2와 같다.



(그림 2) 사이버 거점을 활용한 위협탐지 과정 체계도

4. 실험 및 결과

본 논문에서 사이버 거점 위협탐지는 크게 두 가지로 분류한다. 첫 번째는 침해사고가 발생한

2) 엔드포인트(Endpoint)는 컴퓨터와 모바일, 서버 등 단말을 말한다. 정보보안에서는 엔드포인트에서 발생하는 악성행위를 실시간으로 감지하고 이를 분석 및 대응하여 피해 확산을 막는 것을 엔드포인트 탐지 및 대응(Endpoint Detection and Response, 줄여서 EDR)이라고 함.

3) 미디어(신문, 잡지, 라디오, 텔레비전 등), 인터넷(블로그, 다크웹, 웹사이트, YouTube, Twitter, Facebook 등), 공공 정부 자료(공공 정부 보고서, 연설, 컨퍼런스 등), 전문 및 학술 간행물(저널, 학술 논문, 기고문 등), 상업자료(상업용 이미지, 재무 및 산업 평가 등), Gray Literature (기술 보고서, 사전 인쇄, 특허, 비즈니스 문서 등)

후에 조사분석 과정에서 침해지표를 획득하거나 타 기관으로부터 공유받는 수동적 방법이다. 두 번째는 적극적으로 직접 적대적 해킹그룹의 거점을 찾아서 감시하는 능동적 방법이다.

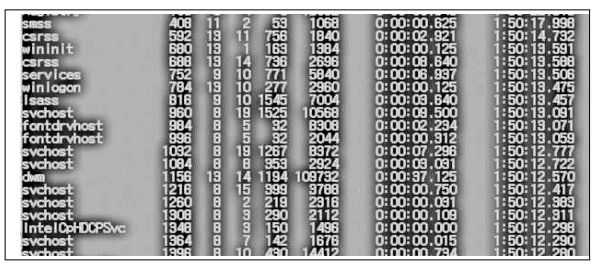
4.1 수동적 사이버 거점 위협탐지

수동적 위협탐지 방법 중에서 첫 번째는 침해사고 발생 후 조사분석을 통해 공격자의 정보를 획득하는 것이다. 침해사고가 발생하면 여러 가지 명령어 및 분석 도구를 사용하여 공격 경로, 공격자 정보, 피해 정도를 확인한다. 먼저 명령어를 통해 시스템 내에 존재하는 정보를 수집한다.

(그림 3) 네트워크 상태

위 그림 3과 같이 시스템에서 기본적으로 제공하는 명령어를 통해 네트워크 상태를 확인할 수 있다. netstat 명령어는 윈도우와 리눅스에서 사용하며, 현재 로컬 주소와 연결된 외부 주소 및 연결 상태(ESTABLISHED 등)가 출력된다(로컬 주소는 보안상 제외). 위 그림에 나타난 외부 주소 20.198.162.78 IP가 싱가폴의 데이터센터 IP로 공격자의 IP주소로 판단된다.

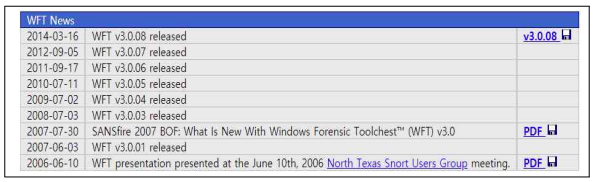
공격자는 하나의 악성코드를 반복 사용하므로 프로세스 목록을 통해 악성코드를 확인한다면, 차후 동일 또는 유사한 공격에 대비할 수 있다.



(그림 4) 프로세스 목록

그림 4는 오픈소스 도구 pslist를 사용하여 출력한 화면이다. 프로세스 목록에서 이름이 의심스러운 프로세스를 식별할 수 있고, Pid(프로세스 id)로 프로세스 사이의 관계를 확인할 수 있다. 평소 정상 상태에서 사용하는 프로세스 목록을 관리하고 있다면 의심스러운 프로세스를 쉽게 식별할 수 있다. 또한 부모 프로세스가 없는 좀비 프로세스는 더욱 유심히 살펴볼 필요가 있다. 위 그림에서 같은 svchost 프로세스명이 다수 식별된다. 이는 윈도우 기본 프로세스인 svchost의 이름을 도용하여 악성코드를 위장하는 대표적인 방식이다.

네트워크, 프로세스 정보 외에도 명령어 및 도구를 사용하여 시스템 계정정보, 원격 접속 로그 등을 확인할 수 있으며, Windows Forensic Toolchest(WFT) 에서는 그림 5와 같은 자동화된 도구를 제공하고 있다[24].



WFT News		
2014-03-16	WFT v3.0.08 released	v3.0.08
2012-09-05	WFT v3.0.07 released	
2011-09-17	WFT v3.0.06 released	
2010-07-11	WFT v3.0.05 released	
2009-07-02	WFT v3.0.04 released	
2008-07-03	WFT v3.0.03 released	
2007-07-30	SANSfire 2007 BOF: What Is New With Windows Forensic Toolchest™ (WFT) v3.0	PDF
2007-06-03	WFT v3.0.01 released	
2006-06-10	WFT presentation presented at the June 10th, 2006 North Texas Snort Users Group meeting.	PDF

(그림 5) 윈도우 포렌식 자동화 도구

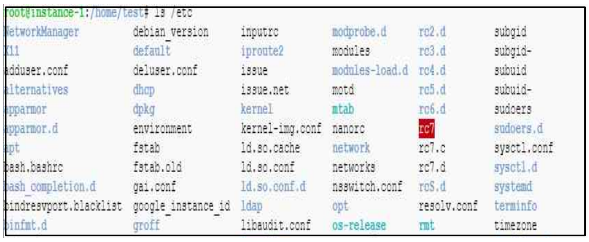
두 번째 수동적 위협탐지 방법으로는 타 기관으로부터 침해지표를 공유받는 것이다. 한국인터넷진흥원(KISA)에서 운영하는 C-TAS가 대표적인 사이버 위협정보 분석공유 시스템이다[25]. C-TAS는 국내외 기업 및 기관들과 사이버 위협의 지능화·고도화로 인한 침해사고 조기 대응과 피해확산 방지를 위해 구축되었다. 또한, 여러 산업 분야에 걸쳐 광범위하게 발생하고 있는 다양한 사이버 위협정보를 기관과 기업 등에 상호 공유하는 시스템이다. 이러한 위협 공유 시스템은 참여기관이 많을수록 신뢰도가 높아진다.

4.2 능동적 사이버 거점 위협탐지

능동적 위협탐지는 정보 수집에 대한 실험을 시나리오 통해 구현한다. 적대적 해킹그룹은 소속이 특정되는 상황을 회피하기 위해 C&C 서버로 공용 클라우드 서버를 사용할 것이며, 또 다른 공격자가 해당 서버에 백도어를 설치하고 정보를 획득하는 시나리오로 진행한다. 백도어를 설치한 공격자는 사회 공학적 기법

등을 사용하여 공격 대상 C&C 서버의 IP와 원격 접속 포트 및 root 비밀번호를 획득하였다고 가정한다.

아래 그림 6과 같이 C&C서버의 etc 폴더 아래 다양한 파일들이 존재한다. 공격자는 서버 관리자의 감시를 회피하기 위해 다른 파일들과 이름이 유사한 'rc7' 이라는 백도어 파일을 만들었다.



(그림 6) C&C 서버의 /etc/ 폴더에 위장된 백도어

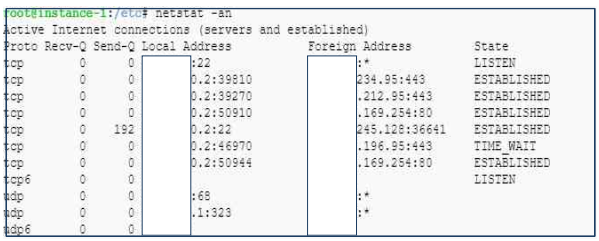
'rc7' 이라는 백도어 파일을 만든 이후에는 root 계정의 비밀번호가 변경되더라도 백도어 파일을 통해 언제든지 root 권한을 획득할 수 있다. 아래 그림 7은 백도어 실행 전과 후의 권한 변경 화면이다.

백도어 실행 전 (임시로 생성한 test 권한)	$ whoami
	test
	$ id
	uid=1001(test) gid=1002(test) groups=1002(test)
	$

백도어 실행 후 (root 권한 획득)	root@instance-1:/etc# whoami root root@instance-1:/etc# id uid=0(root) gid=0(root) groups=0(root),1002(test) root@instance-1:/etc#

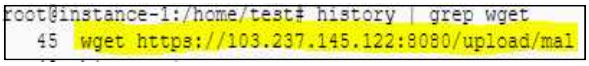
(그림 7) 백도어 실행 전과 후의 권한 변경

백도어를 통해 C&C 서버의 권한을 획득한 공격자는 해킹그룹의 활동을 모니터하면서 다양한 정보를 획득할 수 있다. 아래 그림 8은 해당 C&C 서버의 네트워크 연결상태 화면이다. 네트워크가 연결된 상태에서 표시되는 IP주소를 조사하여 해킹그룹의 주요 활동 영역을 파악할 수 있을 것이다.



(그림 8) netstat 명령어로 네트워크 연결상태 확인

또한 C&C 서버에서 입력된 명령어를 확인하여 해킹그룹의 활동을 파악할 수 있다. 예를 들어 아래 그림 9와 같이 특정 IP에 접근하여 악성코드로 추정되는 파일 다운로드 행위가 식별되었다면 해당 IP에 대한 추가적인 조사가 필요하다.



(그림 9) C&C 서버에서 해킹그룹의 활동 확인

해당 IP는 평판 조회 결과에 따라 베트남의 또 다른 클라우드 서버에서 사용하는 IP이며, 최근 악성 행위 수행 기록이 다수 확인된 IP이다. 이러한 경우에 거점을 확보한 해킹그룹과 해당 베트남 클라우드 서버를 사용하는 해킹그룹은 동일 해킹그룹이거나 최소한 협력 관계에 있다는 사실을 파악할 수 있다.

(그림 10) 의심스러운 IP의 평판 조회 결과

5. 결론

본 논문에서는 사이버 거점을 활용한 위협탐지 모델을 제안하였다. 방어 관점에서 이 모델은 기존의 수동적인 사이버 위협을 탐지하는 방법에서 능동적인 방법으로 개선하였다. 이를 통해 해킹 위협으로부터 조직의 자산을 보호하고 방어 효율을 향상할 수 있을 것이다.

제안 모델은 실제 국방 환경에서 실험하여 실효성을 검증하였다. 특히, 사이버 거점을 활용한 위협탐지는 수동적 방법과 능동적 방법으로 구분하여 실험하였다. 그리고 제안한 방법은 적대적 해킹그룹의 위협에 대응하는 하나의 접근방법이다. 이를 기반으로 기관이나 기업의 환경을 고려한 적용과 성과로 이어지길 기대한다.

향후 과제로, 첫 번째는 직접 사이버 거점 정찰 수행에 필요한 법적 검토이다. 두 번째는 조직적인 해킹그룹의 정체를 식별하는 방법 연구가 필요하다. 세 번째는 사이버 위협을 탐지하고 축적하여 다양한 분석과 위협정보를 생산하는 방안이 연구되어야 할 것이다.

참고문헌

[1] McMillan R. Definition: threat intelligence. Gartner; 2013. https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf.

[2] Chrismon D, Ruks M. Threat Intelligence: Collecting, analyzing, evaluating, MWR Infosecurity, UK Cert, United Kingdom; 2015. https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf.

[3] Dalziel H. How to define and build an effective cyber threat intelligence capability. Syngress Publishing of Elsevier; 2014. https://www.sciencedirect.com/book/9780128027301/how-to-define-and-build-an-effective-cyber-threat-intelligencecapabilit.

[4] Nenekazi N. P. Mkuzangwe, Zubeida C. Khan, "Cyber-Threat Information-Sharing Standards: A Review of Evaluation Literature", The African Journal of Information and Communication(AJIC) On-line version vol.25 Johannesburg 2020. DOI:http://dx.doi.org/10.23962/10539/29191.

[5] Md. Farhan Haque, Ram Krishnan, "Toward Automated Cyber Defense with Secure Sharing of Structured Cyber Threat Intelligence", Information Systems Frontiers 2021 - Springer, DOI:https://doi.org/10.1007/s10796-020-10103-7.

[6] Se-Ho Lee, In-June Jo, "Proposal of Security Orchestration Service Model based on Cyber Security Framework", The Journal of the Korea Contents Association Vol.20, No.7, pp.618-628, 2020. https://doi.org/10.5392/JKCA.2020.20.07.618.

[7] Jae-Hyun Choi, Hoo-Jin Lee, "A Study on the Real-time Cyber Attack Intrusion Detection Method", Journal of the Korea Convergence Society Vol. 9. No. 7, pp. 55-62, 2018. https://doi.org/10.15207/JKCS.2018.9.7.055.

[8] Alper Caglayan, Mike Toothaker, Dan Drapeau, Dustin Burke & Gerry Eaton, "Behavioral analysis of botnets for threat intelligence", Information Systems and e-Business Management Vol. 10, pp.491-519, Dec. 2012. https://doi.org/10.1007/s10257-011-0171-7

[9] Fireeye Mandiant, "what is cyber threat intelligence", DOI:https://www.fireeye.kr/mandiant/threat-intelligence/what-is-cyber-threat-intelligence.html

[10] Gartner, "Security Threat Intelligence Products and Services Reviews and Ratings", DOI:https://www.gartner.com/reviews/market/security-threat-intelligence-services.

[11] SANS, "The Evolution of Cyber Threat Intelligence(CTI) : 2019 SANS CTI Survey", DOI:https://www.sans.org/white-papers/38790/.

[12] 김경한, 이슬기, 김병익, 박순태, "OSINT기반의 활용 가능한 사이버 위협 인텔리전스 생성을 위한 위협정보 수집 시스템", 정보보호학회지, pp. 75-80, 제29권 제6호, Dec. 2019. DOI:https://www.koreascience.or.kr/article/JAKO201904533932647.pdf.

[13] SSeung-Soo Nam, Chang-Ho Seo, Joo-Young Lee, Jong-Hyun Kim, Ik-Kyun Kim, "Context cognition technology through integrated cyber security context analysis", Journal of Digital Convergence Vol. 13, No 1, pp.313-319, Jan, 2015. DOI : https://www.earticle.net/Article/A239116.

[14] Kim Namuk, Eom Jungho, "Attack Path and Intention Recognition System for detecting APT Attack", Journal of Korea Society of Digital Industry and Information Management, Vol. 16. No. 1, pp. 67-78, 2020. DOI: https://doi.org/10.17662/ksdim.2020.16.1.067.

[15] Lim Changwan, Shin Youngsup, Lee Dongjae, Cho Sungyoung, Han Insung, Oh Haengrok, "Real-time Cyber Threat Intelligent Analysis and Prediction Technique", KIISE transactions on computing practices Vol.25, No.11, pp.565-570, 2019. DOI : 10.5626/KTCP.2019.25.11.565.

[16] Han Choong-Hee, Han ChangHee, "Cyber threat Detection and Response Time Modeling", Journal of Internet Computing and Services, Vol.22, No.3, pp.53-58, Jun. 2021. https://doi.org/10.7472/jksii.2021.22.3.53.

[17] Se-Ho Lee, In-June Jo, "Proposal of Security Orchestration Service Model based on Cyber Security Framework", The Journal of the Korea Contents Association Vol.20, No.7, pp.618-628, 2020. https://doi.org/10.5392/JKCA.2020.20.07.618.

[18] Jae-Hyun Choi, Hoo-Jin Lee, "A Study on the Real-time Cyber Attack Intrusion Detection Method", Journal of

the Korea Convergence Society Vol. 9. No. 7, pp. 55-62, 2018. https://doi.org/10.15207/JKCS.2018.9.7.055.

[19] 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.

[20] T. Mattern, J. Felker, R. Borum, G. Bamford, "Operational Levels of Cyber Intelligence", International Journal of Intelligence and Counterintelligence, 27 : 702 - 719, 2014. https://doi.org/10.1080/08850607.2014.924811.

[21] ENISA, “Threat Landscape Report 2016”, European Union Agency for Cybersecurity (ENISA), Jan. 2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

[22] https://ichi.pro/ko/cti-cyber-threat-intelligence-yoyag-1-124932966514066.

[23] Jongwon Choi, Yesol Kim, Byung-gil Min, “A Study on ICS Security Information Collection Method Using CTI Model”, Journal of The Korea Institute of Information Security & Cryptology Vol.28, No.2, pp.471-484, Apr. 2018. DOI:10.13089/JKIISC.2018.28.2.471.

[24] http://www.foolmoon.net/security/wft/index.html, “Windows Forensic Toolchest”, (검색일: 2021.12.23.).

[25] https://www.krcert.or.kr/webprotect/ctas.do, “사이버 위협정보 분석공유(C-TAS) 시스템”, (검색일: 2021.12.23.).

[26] 엄정호, “모자이크전 수행 개념을 적용한 능동형 상황 탄력적 사이버 방어작전”, 융합보안논문지, 21(4), pp.41-48, 2021.

〔저자소개〕

김 인 환 (Inhwan Kim)
1989년 2월 금오공과대학교 공학사
1997년 2월 일본 게이오대학교 공학석사
2022년 2월 강릉원주대 소프트웨어학과 공학박사
2022~현재 세종대학교 컴퓨터공학과 대우교수
email : ihkim@sejong.ac.kr

강 지 원 (Jiwon Kang)
1988년 2월 금오공과대학교 공학사
1997년 2월 연세대학교 컴퓨터과학 (정보보호 전공) 석사
2012년 8월 경기대학교 정보보호학 박사
2017년 9월~현재 세종대학교 컴퓨터공학과 산학협력중점교수
email : jwkang@sejong.ac.kr

안 훈 상 (Hoonsang An)
1987년 육군사관학교 공학사
1998년 美 네브라스카 주립대학교 전산학과(공학석사)
2016년 아주대학교 NCW학과 (박사수료)
2022~현재 강릉원주대 박사과정
email : husker@naver.com

전 병 국 (Byungkook Jeon)
1985년 광운대 전산과(이학사)
1991년 광운대학교 컴퓨터과학과 (이학석사)
2000년 광운대학교 컴퓨터과학과 (이학박사)
1991~1993년 KISTI 연구원
1993~현재 강릉원주대 교수
email : jeonbk@gwnu.ac.kr