정 보 보 호 학 회 지
제 31 권 제5호, 2021. 10

사이버 위협 인텔리전스 환경에서의 종합분석 전략

이 슬 기*, 김 동 욱*, 김 병 재*, 이 태 우*, 한 상 원*, 이 재 광*

요 약

한국인터넷진흥원 종합분석팀은 사이버 위협 인텔리전스(CTI)를 통해 주요 침해사고를 추적하여 분석하고 이에 대한 대응방안을 마련, 공유하는 역할을 수행하고 있다. 구체적으로는 외부 협력채널 혹은 기존 사고에서 사용된 악성도구의 흔적을 기반으로 악성 인프라를 탐지하고, 이에 대한 공격자의 전략을 상세히 분석, 정리한 보고서를 발간하여 기업의 보안 수준을 제고하려 노력하고 있다. 본고에서는 사이버 위협 인텔리전스 측면에서 변화한 종합분석의 관점 및 역할을 소개하고, 고도화되어가는 침해사고를 대응하기 위한 향후 전략을 제안한다.

Ⅰ. 서 론

한국인터넷진흥원은 침해사고가 발생하고 방어자가 피해를 인지, 신고한 이후에 대응하는 전통적 침해사고 대응을 개선하려 노력하고 있다. 피해인지 시점을 앞당겨 대응시간을 축소하고, 보다 상세한 분석결과 제공을 통해 대응수준을 제고하고 있다. 이와 더불어, 사고 발생 이후 침해사고 재발 위험을 경감하기 위한 방안을 안내하는 등 사후조치를 통해 기업의 보안성 향상을 지원하고 있다.

전통적 의미의 침해사고 대응은 침해사고 발생 이전을 고려하지 않지만, 사고 발생 이전에 작용할 수 있는 여러 요소들이 존재한다. 첫 번째는 사고가 발생할 수 있는 지점인 기업의 보안 현황을 미리 점검하고 훈련하는 것이다. 한국인터넷진흥원의 여러 사업 중 내 PC 돌보미와 사이버 위기대응 모의훈련이 대표적이다. 두 번째는 보다 능동적인 정보수집 및 탐지이다. 오픈소스 인텔리전스(Open-source Intelligence)와 기관 차원에서 구축한 협력채널을 통해 능동적으로 위협정보를 수집하고 탐지, 대응에 나서고 있다. 세 번째는 침해사고 발생 이전에 잠재적으로 확인 가능한 전조현상이다. MITRE ATT&CK™에서는 PRE 단계로 정찰(Reconnaissance)과 자원 개발(Resource Development)을 포함하고 있다. 정찰 단계는 공격 대상을 선정하는 것을 포함하여 대상의 정보를 수집하는 행위를 의미한다. 또한, 자원개발은 침해사고 수행을 위해 직접적으로 사용되는 도구의 개발 및 정보유출과 명령제어를 수행하기 위한 인프라를 구축, 확보하는 단계를 의미한다. ATT&CK 프레임워크의 PRE 단계처럼 공격자는 침해사고 수행을 위해 사전 준비가 필요하며, 이로 인해 발생 가능한 위험을 사전에 식별하려는 노력이 필요하다.

한국정보통신기술협회(TTA)에서는 사이버 위협 인텔리전스(Cyber Threat Intelligence; CTI)를 사이버 시스템의 안전을 위협하는 정보를 수집하여 상황을 분석하고 사이버 보안 위협에 효과적으로 대응하는 방법이라고 정의하고 있다[1]. 한국인터넷진흥원 종합분석팀은 사이버 위협 인텔리전스의 관점에서 선제적으로 위협을 헌팅하고 상세분석, 최종적으로 리포트를 배포하여 기업이 적용 가능하도록 공유하고 있다. 본고에서는 구체적인 위협 대응 현황과 변화하는 사이버 환경을 준비하는 전략을 제시한다.

우선, 외부 채널 및 자체 수집을 통해 확보한 위협을 분석하여, TTPs 보고서로 공유하는 과정을 2장에서 설명한다. 3장에서는 자체 개발한 AI 프로파일링 분석시스템을 소개하고, 마지막으로 네트워크 분석을 통한 위협관리 전략에 대하여 제안한다.

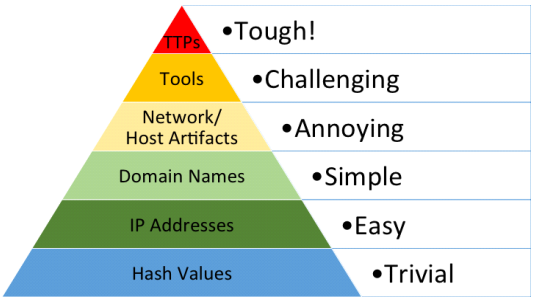
* 한국인터넷진흥원 (선임연구원, sglee@kisa.or.kr; 선임연구원, kimdw777@kisa.or.kr; 선임연구원, kimbyeongjae@kisa.or.kr; 선임연구원, heavyrain@kisa.or.kr; 선임연구원, hsw89@kisa.or.kr 팀장, leejk@kisa.or.kr)

Ⅱ. TTPs 보고서

2.1. TTPs 필요성 및 의미

TTPs 보고서라는 이름으로 외부 공개되는 보고서는 TTPs(Tactics, Techniques, and Procedures)의 정의에서 출발한다. TTPs는 특정한 공격자가 수행한 APT 공격을 프로파일링하여 산출한 해당 공격자가 사용하는 전략과 전술, 그 과정을 의미한다. 과거에는 IoCs(Indicators of Compromise)라는 침해지표를 활용하여 신속한 공유를 통해 악성 인프라를 차단하였으며, 이 방법은 지금도 유효하다. 하지만, IoCs는 공격에 악용된 악성코드의 해시 값과 IP주소, 도메인 주소, URL 등 특정한 단일 개체를 의미하며, 변화하는 공격 인프라에 대응하기 어렵다는 단점이 있다. 예를 들어, 악성코드 내부에 존재하는 명령제어 서버주소만 변경하더라도 악성코드 해시는 변화하며, 공격에 악용되는 도메인 주소도 계속해서 변화한다. 따라서 IoCs를 통한 대응은 후행성을 지닐 수밖에 없다.

TTPs는 IoCs와 달리, 공격자가 지니는 특성이 드러날 수 있는 정보이다. 공격을 수행하기 위하여 습득한 지식 및 도구, 해킹 그룹이 가지는 전략 등이 침해사고에 자연스레 투영되기 때문에 TTPs를 도출하게 되면 해당 시점의 공격자는 상세하게 분석되었다고 말할 수 있다. 공격자는 사전에 준비한 악성도구와 취약점을 활용하기 위해 사용법을 학습한다. 마찬가지로 공격을 수행하는 목적이 지속된다고 가정할 때, 공격 타겟군이 유사할 것이며, 최종적으로 수행하는 악성행위(랜섬웨어, 정보유출, 시스템 파괴 등) 또한 유사할 것이다. 그리고 이러한 공격자의 특성들은 내재화되어 있기 때문에 변화하기 어렵다. 변화하기 어려운 지점을 도식화한 것이 그림 1의 '고통의 피라미드'이다[2].



〔그림 1〕 고통의 피라미드(The Pyramid of Pain)

서로 다른 시점과 타겟에서 발생한 침해사고를 동일한 그룹이 수행하였다고 발표하는 경우, IoCs 레벨에서 완전히 일치하는 경우도 존재하지만 TTPs를 근거로 판단하는 경우가 대다수이다.

동일한 공격그룹을 추적하는 것 이외에 기업에서도 IoCs가 아니라 TTPs를 적용하는 것이 효과적이다. 변화하는 IoCs를 계속 추가하여 보안환경을 운영하기에는 시스템에 부하가 발생할 수도 있으며, 단발성으로 차단하는 것이 비효율적이기 때문이다. 공격자의 최근 TTPs를 기업에 적용할 수 있다면, 변화하는 공격 인프라를 계속해서 방어할 수 있다. 이러한 변화가 기업에 적용되기 위해서는 피해 발생 시 높은 위험성을 가지면서 라이브한 TTPs 공유가 필요하다.

활용 가능한 TTPs를 도출하기 위해서는 많은 리소스가 수반되며 동시에 많은 제약사항이 존재한다. 우선, 라이브한 침해사고에 대한 접근권한이 필수적이다. 이를 위해서는 실제 피해가 발생한 기업 및 피해기업과 협력 중인 보안업체 혹은 한국인터넷진흥원 등이 가능할 것이다. 또한, 발생한 사고를 프로파일링할 수 있는 분석 역량이 필수적이다. 마지막으로 이 분석결과를 가공하여 공유하는데 발생하는 리소스에 대한 보상 문제가 존재한다. 모든 사례에 해당하지는 않지만, 보안업체에서는 계약한 업체에 특화된 TTPs를 공유함으로써 사업화를 진행하고 있으며, 한국인터넷진흥원은 공공성을 띄기 때문에 범용 적으로 활용 가능한 리포트를 무상으로 공개하고 있다.

모든 공격자의 TTPs를 분석하여 공유하는 것이 이상적이지만, 인적 리소스 제한 등 현실적인 문제로 인해 분석 대상을 선정하는 것이 중요하다. 그리고 분석대상은 우리나라 기업에 가장 위협을 주는 공격 그룹이 되어야 한다. 따라서 한국인터넷진흥원 종합분석팀은 TTPs를 도출하는데 있어 특정한 공격자를 선정하지 않고, 기업을 빈번하게 공격하는 공격자를 추적하여 TTPs를 분석한다.

분석의 시작점은 공격자가 아니라, 보호해야할 기업이다. 구체적으로는 민간 기업의 침해사고를 조사하는 역할을 수행하기 때문에 분석대상 선정은 자연스레 진행될 수 있다. 혹은 사고 량이 적더라도 피해예상액이 크거나 기술적으로 공유가 필요한 경우 대상으로 선정할 수 있다. 발생한 피해기업에서 TTPs를 도출하면, 라이브하기 때문에 기업의 활용성이 높다

는 장점이 존재한다. 또한, 이 외에도 민·관·군 협력 등을 통해 수집된 정보를 이용하여 주요 사고를 선정하기도 한다.

2.2. TTPs 분석 사례

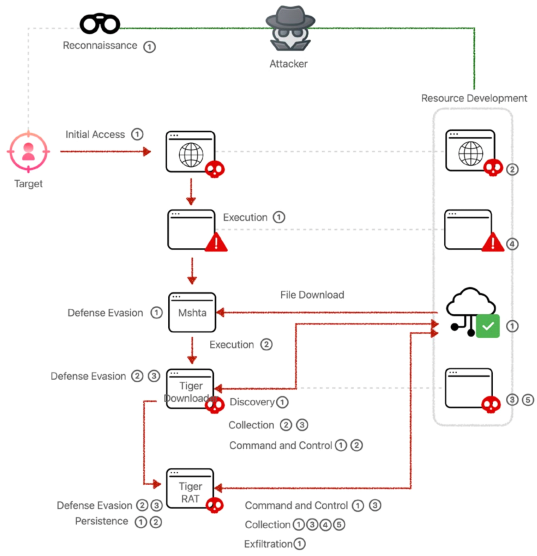
TTPs 보고서는 2020년 4월부터 시작하여 6편(2021년 10월 기준)까지 발간되었다. 하지만, TTPs의 중요성을 해당 시점에 인지하고 전환한 것이 아니라 과거부터 점차 변화한 것이다. 그림 1과 같은 개념이 공격자에게 어떠한 위협으로 다가오는지에 대한 고민은 과거부터 존재하였으며, 급변하는 공격을 대표할 수 있는 보고서의 필요성이 내부적으로 요구되고 있었다.

다음은 한국인터넷진흥원에서 2021년 9월에 발표한 '타겟형 워터링홀 공격전략 분석' 보고서를 간략히 소개한다[3]. 국내 주요 기업의 홈페이지를 해킹하여 악성코드를 삽입, 특정 타겟이 해당 홈페이지에 접근하였을 때 악성코드를 다운로드받아 실행하는 타겟형 워터링홀 공격 전략이 사용된 침해사고이며, 그림 2는 Operation ByteTiger로 명명한 침해사고의 공격 개요도를 도식화한 결과이다. 감염된 홈페이지로 접근한 공격대상은 특정 소프트웨어의 취약점으로 인하여 윈도우 유틸리티 중 하나인 mshta.exe가 실행되고 자동으로 악성코드를 다운로드, 실행하게 된다. 이후 커맨드라인 명령어로 정보수집, 지속적인 공격을 위한 스케줄러 및 레지스트리 등록이 진행된다.

공격자가 새로 개발한 것으로 보이는 TigerRAT와 TigerDownloader는 Base64, RC4, DES 등의 인코딩, 암호화가 수행되었다. TigerRAT은 파일 검색, 키로깅, 스크린 캡쳐 등 감염된 단말기의 정보를 송수신하며, TigerDownloader는 파일 업로드·다운로드를 메인 기능으로, 명령어를 실행하는 악성코드이다.

Operation ByteTiger는 특정 제품의 취약점을 악용하였기 때문에 공격대상의 환경을 사전에 알고 있었을 것으로 예상되며, 공격대상이 자주 접근하는 홈페이지에 악성 스크립트 및 익스플로잇을 삽입하는 특징을 보이기 때문에 공격대상을 선별, 명확한 목표를 가지고 해킹공격을 수행했다고 판단할 수 있다.

또한, 해당 보고서에서는 핵심 악성코드의 동작을 상세히 분석하고, 유사한 침해사고를 분석한 해외 보고서의 정보를 비교 분석하여 변화하는 공격자의 전략을 소개하였다.



〔그림 2〕 Operation ByteTiger 공격 개요도[3]

2.3. TTPs 분석결과 활용

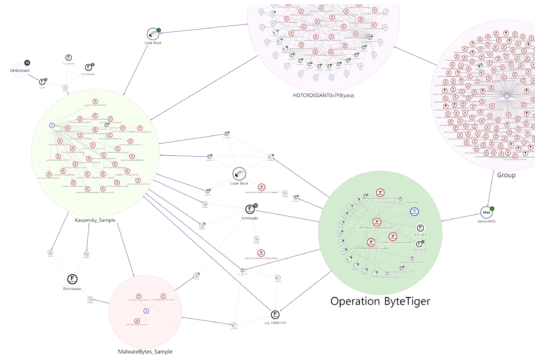
각 기업에서는 한국인터넷진흥원을 포함하여 공개되는 TTPs를 적용하면 최근 위협이 되는 공격에 효과적으로 대응할 수 있다. 모든 기업마다 구성환경이 상이하기 때문에 TTPs 보고서에서 구체적인 룰셋을 제공하기는 어렵다. IoCs와 달리 즉시 적용할 수 있는 형태로 제공되지 않기 때문에 기업에서는 각자 환경에 적합한 형태로 가공, 적용해야하는 어려움이 존재하고, 적용방안을 각자 마련해야 한다. TTPs를 발표하는 주체는 기업이 적용하기 쉬운 형태로 공개하려 고민하고, TTPs를 수용하는 기업·기관도 마찬가지로 자사의 환경을 이해하고 적용하려는 노력을 기울인다면, 이해의 차이를 줄일 수 있을 것이라 기대한다.

TTPs 보고서는 피해기업의 정보가 노출되지 않도록 IoCs 레벨의 정보를 마스킹하여 공개하고 있다. 따라서 보고서를 어떻게 적용해야하는 지에 대한 어려움이 존재할 것이다. 예를 들어 2.2 TTPs 분석 사례에서 소개한 공격 전략의 경우 공격거점으로 악용된 서버를 공개하지는 않지만, 거점 서버에 탑재되어 운영된 웹페이지의 동작은 상세하게 서술한다. 기업은 특정한 IoCs에 접근하지 않도록 제어 규칙을 정의하는 것이 아니라, 내부 통신을 통해 어떠한 트래픽이 발생

하는지를 확인하고 자체 규칙을 생성해야 한다. 네트워크 뿐 아니라 이벤트, 레지스트리 또한 마찬가지이다. 기업이 보유한 장비의 점검범위를 고려하여 규칙을 생성하고, 최신 공격에 대한 지속적인 관심을 통해 룰 셋 업데이트가 필요하다.

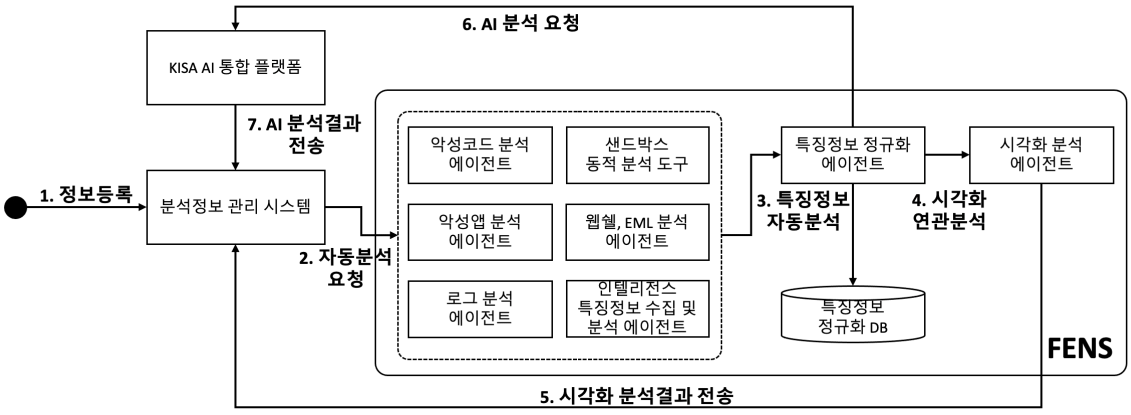
Ⅲ. FENS(AI 프로파일링 분석시스템)

침해사고가 발생하고 대응하는데 있어 분석가의 역량에 모든 결과가 좌우되던 환경이 분석 자동화 기술의 발전으로 변화하고 있다. 특히, 인공지능의 기술의 발전은 적재되던 악성코드 및 사고분석 결과를 활용할 수 있게 되었다. 지능화와 더불어 대량화로 확산되는 침해사고 대응을 한정된 분석 리소스로 대응하기에 어려움이 있으며, 대응하더라도 발생하는 사고의 량이 대응역량을 초과하는 순간 사회에 혼란을 야기할 수 있다. 또한, 한국인터넷진흥원에서 분석가들이 오랜 기간 분석한 결과 데이터는 누적되고 있으나, 실질적으로 사고를 분석함에 있어서 어떻게 활용해야 하는 지에 대한 고민이 부족하였다. 한국인터넷진흥원은 이러한 자동화된 분석 혹은 분석 지원도구, 데이터 활용의 필요성으로 인해 FENS(Feature Engineering Normalization System)를 개발하여 내부적으로 활용하고 있다. 자동분석, 특징정보 추출 및 정규화, 시각화 분석 등 세 가지 범주로 대표 기능이 구현되어 있으며, 해당 시스템을 활용하여 TTPs 6번 보고서가 발간되었다. 그림 3은 FENS의 외부 시스템(AI 통합 플랫폼, 분석정보 관리 시스템 등)과의 연동 및 최초 악성코드·침해사고가 접수되었을 때, 자동으로 동작하는 흐름을 도식화한 그림이다.



〔그림 4〕 공개정보와 결합한 FENS 분석결과〔3〕

공개된 악성 도구를 악용하거나 획일화된 공격 전략이 사용된 해킹공격은 많은 부분 자동화된 분석 결과에 의하여 해석이 가능하다. FENS를 통해 산출한 결과는 한국인터넷진흥원 내부의 다른 시스템과 연계하여 분석결과를 재활용하며, 분석가도 마찬가지로 시각화 시스템 등을 통해 악성코드가 기존 수집된 정보와 어떠한 연결 관계에 있는지 한눈에 파악이 가능하다. 그림 4는 국외(Kaspersky, Malwarebytes)에서 발표한 정보와 TTPs 6번 보고서에서 다룬 침해사고에서 확보한 정보를 비교한 시각화 분석 결과이다[3]. Operation ByteTiger에서 자동으로 추출한 코드블록, 리치헤더 등이 특징을 공통으로 공유하고 있기 때문에, 접수되는 악성 샘플의 중요도가 높다고 판단할 수 있다. 이러한 기능을 통해 분석가는 대량의 악성행위 중 우선으로 분석할 대상을 결정할 수 있다. FENS를 통해 고위험 침해사고를 신속하게 식별하고 분석정확



〔그림 3〕 FENS 내부 구성 및 동작 개요도

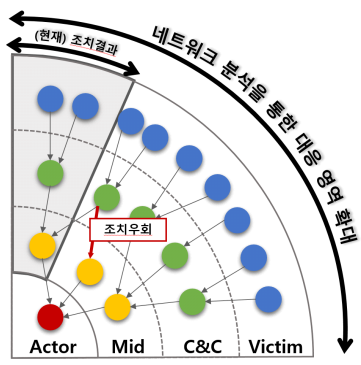
도를 향상시킬 수 있기 때문에 고위험 침해사고에 대한 선제적 대응을 기대할 수 있으며, 분석결과로 누적되는 고품질의 대용량 데이터로 인해 FENS의 활용성이 자연스레 높아질 것으로 예상된다.

Ⅳ. 네트워크 인텔리전스

현재 호스트 레벨에 존재하는 인프라(악성코드, 사고정보) 분석을 통해 프로파일링을 수행하고 결과를 발표, 정리하고 있다. 내부자 소행 및 물리적 접속을 제외하고 거의 모든 침해사고는 네트워크를 통해 침투, 내부 장악, 악성행위 수행 등의 절차로 전개된다. 따라서 보안장비가 존재한다면, 장비로 기록된 로그파일을 통해 접속지점을 파악하고, 어느 지점으로 침투했는지를 확인, 해당 단말기를 조사하는 순서로 분석이 진행된다. TTPs 6번 보고서와 같이 타겟형 워터링홀 공격과 그 외에 스피어피싱과 같은 다른 침투방식이 존재하는데, 상대적으로 보다 휘발성인 네트워크 정보는 분석이 용이하지 않다.

대형 침해사고가 발생하기 이전에 네트워크 레벨에서 전조 증상이 발견될 수 있다. 공격자의 특성에 따라, 일반 서버를 공격하거나 정상적으로 임대하는 형식으로 공격 인프라를 저마다의 방식으로 구성하고 있다. 또한, 서버가 존재하는 국가 및 서비스 종류 등에 따라 다양한 형태로 구성되며, 인프라 구성 원칙에 따라 일정기간 동일한 구성 전략을 사용하며 전략 폐기 후 향후 재사용하는 경향을 보인다. 그림 5는 특정 공격자가 APT 공격을 수행하기 위하여 다계층으로 네트워크 인프라를 구성한 도식이다. 최종적인 공격 대상인 피해자(Victim)와 현실세계에 위치한 공격행위자(Actor)를 배제하고 사이버 환경에서 접근 가능한 제어·중계기(Mid, C&C 등) 또한 마찬가지로 대부분 피해자에 속한다. 다만, 피해자가 최종 공격목표 대상인지의 여부 및 공격자의 활용 목적에 따라 해당 피해서버의 활용성이 정의된다.

지금까지는 호스트 레벨에 존재하는 도구가 네트워크 행위를 수행할 때, 각 인프라에 종속되는 네트워크 행위들을 상세 분석한 결과가 외부로 공유되었다. 예를 들어, 악성코드가 외부로부터 명령제어 메시지를 수신하고, 악성행위를 수행, 최종적으로 특정 파일을 외부로 전송했다고 가정한다면, 악성코드의 한 기능으로서 네트워크 행위가 기술되고 있다. 하지만, 상시 운



〔그림 5〕 침해사고를 위한 네트워크 인프라 구성 예시

용되는 봇넷은 다른 관점에서의 분석이 필요하다.

봇넷에 감염된 좀비PC들은 봇넷을 제어하는 컨트롤러 서버로 지속적인 통신을 시도하며, 공격자의 명령제어에 따라 즉시 악성행위를 수행할 수 있다. 봇넷 운영자는 좀비PC를 확보하기 위하여 광범위한 대역으로 스캔성 질의를 수행하며, 알려진 포트(well-known port)를 통해 수행되는 서비스를 예측, 취약한 버전을 공격하는 스크립트를 사용한다. 이 때, 개발도상국가 또는 프라이버시를 보장하는 국가의 프록시 서버를 이용하는 것이 보편적이다. 국내외에서 대형 봇넷 서비스의 컨트롤러를 지속적으로 감시하고 감염된 기기를 치료하려는 노력을 계속하고 있으나, 방어자의 노력만큼 공격자 또한 회피기술을 고도화하고 있다.

따라서 네트워크 관점에서 분석이 필요하고 이를 인텔리전스 수준으로 가공할 필요가 있다. 종합분석팀은 해외에서 공유하는 봇넷 및 감염기기의 정보를 분석, 그래프 형태로 관리·모니터링하는 방안을 연구하고 있으며, 향후 FENS와 연계하여 호스트·네트워크 레벨의 정보를 종합한 시스템으로 고도화할 예정이다. 네트워크 정보를 결합하였을 때, 대형 침해사고로 이어지는 해킹공격이 어떠한 봇넷군에서 발생하였으며, 과거 발생한 침해사고와의 연관성도 파악할 수 있을 것이다. 이를 통해, 호스트 레벨의 이벤트, 로그, 악성코드 등만으로 프로파일링을 수행하는 것이 아니라 네트워크 단위로도 공격자를 분류하고 핵심 침해사고를 선정할 수 있을 것이라고 기대한다.

V. 결 론

지금까지 한국인터넷진흥원 종합분석팀이 변화하는 사이버 환경 속에서의 사이버 위협 인텔리전스 전략을 소개하였다. 종합분석팀은 상대적으로 침해사고 경험이 적고, 현재 활동 중인 침해사고 데이터를 확보하기 어려운 기업에게 라이브한 데이터와 APT 공격 그룹의 전략을 공유함으로써, 보안성 강화를 유도하고 있다. 이를 고도화하기 위하여 자체적인 분석역량을 강화함과 더불어, 대량으로 확산되는 침해사고를 자동으로 분석, 지원할 수 있는 시스템 개발을 계속하고 있다.

또한, 공격에 악용되는 인프라를 보다 상세하게 분석할 수 있도록 네트워크 단위의 분석·모니터링 방안을 연구하고 있으며, 네트워크 분석 결과의 검증 및 피드백 반영을 통해 자동화를 검토하고 있다.

향후 네트워크 단에서의 분석을 정규화 및 개발을 통해 FENS에 적용하고, 대응시간 감소 및 대응수준 제고, 사전예방 등 사이버 보안 수준 향상을 위해 프로파일링 결과를 지속적으로 공유할 예정이다.

참 고 문 헌

[1] 한국정보통신기술협회, “사이버 위협 인텔리전스”, 정보통신용어사전, 2021

[2] David J Bianco, “The Pyramid of Pain”, https://detect-respond.blogspot.com/2013/ 03/the-pyramid-of-pain.html, Jan 2014.

[3] 한국인터넷진흥원, “TTPs#6 타겟형 워터링홀 공격전략 분석,” https://boho.or.kr, Sep 2021.

〈저 자 소 개〉

이 슬 기 (Seulgi Lee)
정회원
2013년 2월 : 충남대학교 컴퓨터 공학과 졸업
2019년~현재 : 고려대학교 빅데이터응용및보안학과 석사과정
2012년 10월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 위협 프로파일링, 악성코드, AI 보안, SW 보안

김 동 욱 (Dongwook Kim)
2014년 2월 : 한양대학교 컴퓨터공학과 졸업
2013년 12월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 위협 프로파일링, 코드 분석, 디지털 포렌식, 침해사고 대응

김 병 재 (Byeongjae Kim)
정회원
2011년 2월 : 서울호서전문학교 사이버해킹보안과 학사
2015년 8월 : 동국대학교 디지털포렌식학과 석사
2016년~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 악성코드 분석, 침해사고 대응, AI 보안, 사이버 위협 프로파일링

이 태 우 (Taewoo Lee)
2015년 2월 : 호서대학교 정보보호학과 졸업
2014년 6월~2016년 5월 : 하우리 침해대응센터 연구원
2016년 6월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 사이버 위협 프로파일링, 악성코드 분석, 침해사고 대응

한 상 원 (Sangwon Han)
2014년 2월 : 순천향대학교 정보보호학과 학사
2013년~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 악성코드 분석, 침해사고 대응, AI 보안, 사이버 위협 프로파일링

이 재 광 (JaeKwang Lee)
2007년 2월 : 서울대학교 수학과 석사 졸업
2010년 2월~현재 : 한국인터넷진흥원 인터넷침해대응센터 근무(현 종합분석팀장)
<관심분야> 포렌식, 침해사고 조사기법, 데이터 프로파일링