https://doi.org/10.33778/kcsa.2023.23.4.033

산업기술 유출 방지를 위한 보안 프레임워크 연구

임 양 규*, 박 원 형**, 이 환 수***

요 약

최근 지능형 지속위협(APT) 공격조직은 국가핵심기술을 보유한 기업이나 기관을 대상으로 다양한 취약점 및 공격기법을 악용해서 랜섬웨어를 유포한 후 금전을 요구하거나 국가적으로 중요한 산업기밀 자료를 절취해서 암시장(다크웹)에 유통시키거나 제3국에 판매 또는 기술격차를 줄이는데 활용하는 등 국가차원의 보안대비가 필요하다. 이 논문에서는 Kimsuky, Lazarus 등 한국을 대상으로 APT 공격으로 산업기밀유출 피해를 입혔던 공격조직의 공격수법을 MITRE ATT&CK 프레임워크로 분석하고, 기업의 보안시스템이 추가적으로 갖추어야 할 사이버 보안관련 관리적, 물리적 및 기술적 보안요구사항 26개를 도출하였다. 또한, 보안 요구사항을 실제 보안업무에 활용할 수 있도록 보안 프레임워크 및 시스템 구성 방안도 제안하였다. 이 논문에서 제시한 보안요구 사항은 보안시스템 개발 및 운영자들이 기업의 산업기밀 유출 방지를 위한 보안업무에 활용할 수 있도록 실질적인 방법 및 프레임워크를 제시했으며 향후 이 논문을 기반으로 다양한 APT 공격그룹의 고도화·지능화된 공격을 분석하고 관련 보안대책 연구가 추가적으로 필요하다.

Security Frameworks for Industrial Technology Leakage Prevention

YangKyu Lim*, WonHyung Park**, Hwansoo Lee***

ABSTRACT

In recent years, advanced persistent threat (APT) attack organizations have exploited various vulnerabilities and attack techniques to target companies and institutions with national core technologies, distributing ransomware and demanding payment, stealing nationally important industrial secrets and distributing them on the black market (dark web), selling them to third countries, or using them to close the technology gap, requiring national-level security preparations. In this paper, we analyze the attack methods of attack organizations such as Kimsuky and Lazarus that caused industrial secrets leakage damage through APT attacks in Korea using the MITRE ATT&CK framework, and derive 26 cybersecurity-related administrative, physical, and technical security requirements that a company's security system should be equipped with. We also proposed a security framework and system configuration plan to utilize the security requirements in actual field. The security requirements presented in this paper provide practical methods and frameworks for security system developers and operators to utilize in security work to prevent leakage of corporate industrial secrets. In the future, it is necessary to analyze the advanced and intelligent attacks of various APT attack groups based on this paper and further research on related security measures.

Key words : Cybersecurity, APT, MITRE ATT&CK, Darkweb, Cyber Killchain, North Korea Hacking

접수일(2023년 08월 15일), 수정일(2023년 09월 17일), 게재확정일(2023년 09월 26일)

★ 이 논문은 2023년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0008703, 2023년 산업혁신인재성장지원사업)

* 단국대학교 IT법학협동과정 박사과정

** 성신여자대학교 융합보안공학과 교수

*** 단국대학교 산업보안학과 교수(교신저자)

1. 서 론

최근 산업기밀을 노리는 사이버 공격의 가장 큰 특징은 공격 목표를 집요하게 공격해서 해킹 목표를 달성하는 지능형 지속 위협(APT:Advanced Persistent Threat) 공격이 주를 이루고 있으며 이들 APT 공격조직은 제로데이 또는 패치되지 않은 1-day 취약점을 이용하고, 다양한 기능을 수행하는 악성코드는 기업의 백신 등의 보안시스템에 발각되지 않도록 패킹 및 난독화 기술을 사용하거나 백신의 실시간 탐지를 중단시키는 방법으로 기업의 보안시스템을 우회하여 기업의 네트워크에 침투한다. 침투 이후, 기업의 서버 또는 PC에 랜섬웨어를 유포한 후 복호화 키를 주는 대가로 금전을 요구하거나 기업의 중요 문서 및 회원정보 등의 개인정보를 절취해서 다크웹 상에서 유통시키고 있다. 이러한 일반적인 수준의 자료 외에 방위산업체, 국가핵심기술 보유 기업의 네트워크를 해킹해서 산업기밀을 절취하는 해킹사고는 단순 해킹사고의 측면이 아니라 국가안보 측면에서 접근해야 하는 이유이다.

방위산업체 및 국가핵심기술 보유 연구기관의 해킹 피해사례를 살펴보면, 2021년 6월 발생한 한국항공우주(KAI), 대우조선해양(DSME), 한국원자력연구원은 각각 K-21 설계도면, 원자력추진 잠수함 연구내용 및 소형원자로 개발기술 등의 자료가 탈취된 것으로 추정되는 해킹 피해를 입었다.[13][14]

한편, 이러한 산업기밀유출 사고에 공동으로 대응하기 위한 민·관·학의 공동대응체 중 하나인 민·관·학 신종기술유출 대응 협의회'(의장 강석균, 이하 'TRAT')가 국가정보원과 공동으로 개최한 세미나(2022.12.15.)에서, 국가정보원 산업기밀보호센터 관계자는 "최근 LockBit 3.0 등 랜섬웨어는 기업의 첨단기술 및 영업비밀 데이터를 탈취 후 공개 협박 또는 다크웹 등에서 암거래하는 '산업기밀 탈취 해킹' 형태로 진화했다"고 말했다. 이어, "국내 기업을 노린 귀신(GWISIN) 랜섬웨어의 등장과 글로벌 해킹그룹 랩서스에 의한 국내 제조업 대상 기밀자료 탈취 발생 등 우리 기업도 더는 산업기밀 탈취 해킹에 안전지대가 아니"라며 "산업기밀 탈취 해킹을 차단하기 위해서 기업은 전산보안 강화뿐만 아니라 기술·영업비밀자료의 보호체계 수립, 인력관리 등 산업보안과 융합해 입체적인 대응이 필요하다"고 산업기밀 유출 보안대책의 필요성을 강조 했다.[15]

앞서 살펴본 바와 같이, 다양한 국적 및 목적을 가진 APT 공격조직은 산업기밀자료를 절취하기 위해 지속적으로 공격을 시도하고 있다. 이러한 공격을 분석하는 모델링 기법도 발전하고 있는데, 대표적으로 록히드 마틴社에서 제안한 사이버 킬체인(Cyber Kill Chains)[1][2]과 비영리기업인 마이터(MITRE)에서 제안한 ATT&CK(Adversarial Tactics, Techniques, Common Knowledge) 프레임워크 등이 있다. 본 논문에서는 APT 공격 분석에 적합한 ATT&CK를 활용해서 한국을 대상으로 APT 공격으로 피해를 입혔던 Kimsuky, Lazarus, LAPSUS$ APT 해킹조직의 공격수법을 분석하고, 그에 따른 보안시스템 운영자 또는 보안조직이 추가적으로 수행해야 하는 보안 요구사항을 도출하고 프레임워크를 제안 한다. 대표적인 보안요구사항에는 소속 기업에서 사용중인 시스템의 계정정보 및 탈취당한 문서가 다크웹에서 거래되고 있는지 여부와 쇼단(shodan.io) 등의 시스템 검색엔진에서 소속 기업의 시스템이 공격대상 목표로 노출되어 있는지를 주기적으로 모니터링하고 APT 조직이 보안시스템을 우회하기 위해 사용한 공격기법 중 패턴을 갖는 문자열을 주기적으로 탐지패턴에 추가 후 모니터링하는 방법 등이 있다.

본 논문의 구성은 다음과 같다. 제2장에서는 Lockheed Martin사의 사이버 킬 체인과 MITRE사의 ATT&CK 관련 기본 개념을 살펴보고 제3장에서는 대표적인 APT 공격조직의 공격을 ATT&CK 프레임워크에 맞춰 분석해서 각 조직별 공격전술 및 기술을 비교해 보았으며, 제4장에서는 제3장에서 분석한 결과와 실제 사이버 보안 영역에서 이뤄지고 있는 해킹기법을 조합해서 기업에서 현재 운용중인 보안시스템 또는 보안조직에서 갖추어야 할 추가적인 보안요구사항을 도출하고 산업기밀 유출 방지를 위한 보안 프레임워크를 제안하였다. 마지막

으로 제5장에서는 향후 연구의 발전방향을 서술 한다.

2. 관련 연구

2.1 사이버 킬 체인(Cyber Kill Chain)

사이버 공격을 체계적으로 분석하는 분석 툴은 다양하게 존재하는데, 다양한 분석 툴 중에서 록히드마틴 社가 개발한 사이버 킬체인(Cyber Kill Chain)과 MITRE에서 개발한 ATT&CK가 많이 활용되고 있다.

먼저, 사이버 킬체인은 미국의 방산기업인 록히드마틴 社가 국방 분야에서 사용되는 개념인 킬 체인(타격순환체계)을 사이버 분야에 접목시켜 개발하였다.[1][2]

킬 체인 전략은 1991년 걸프전에 처음 등장했던 용어로, 이라크 군의 스커드 미사일을 방어하기 위한 선제 공격형 방어 전략으로 미사일 발사를 준비하는 정황이 포착되면 선제 공격을 통해 미사일 발사 자체를 저지하겠다는 개념[3]이다. 이후, 2009년에 록히드마틴 社는 자사에 유입되는 다양한 해킹 공격을 분석하고 대응전략을 발표한 백서[2]에서 침입 타격순환체계(Intrusion Kill Chain)이라는 용어로 소개하였고, 이후 사이버 킬 체인이라는 용어로 변경해서 사용하였다. 사이버 킬 체인은 정찰(Reconnaissance), 무기화(Weaponization), 유포(Delivery), 취약점 악용(Exploitation), 설치(Installation), 명령 및 제어(Command&Control), 목적 수행(Actions on Objectives) 등 총 7단계로 구성되어 있다.[4] 사이버 킬 체인을 활용하면 각 단계에서 최대한 신속하게 발견하고 연결고리를 사전에 차단한다면 다음 단계의 진행이 어려워지므로 보안을 유지할 수 있다는 개념이다. 그러나, 사이버 킬 체인은 각 단계에 따른 공격자의 행위를 시간의 흐름에 따라 분석한 것으로 각 단계별로 어떤 기술들이 활용되고 관련된 공격 도구나 해킹그룹 등에 대한 정보와의 연결고리를 파악하기 힘들다는 한계가 존재한다.[5][6]

또한, 외부 침입자만을 공격자로 간주하고 마련한 전략으로 내부자에 의한 침투나 공격자가 이미 내부망에 침투한 경우에는 분석에 한계가 있다. 이는, 사이버 킬 체인에 새로운 전략 혹은 단계의 추가 적용이 필요함을 의미한다.[3]

이에 대한 보완책으로 활용할 수 있는 분석 툴이 MITRE ATT&CK이다.

2.2 MITRE ATT&CK

MITRE ATT&CK는 공격자의 실제 행위를 기반으로 공격 전술정보(Tactics)와 그 목적을 달성하기 위한 공격 기술정보(Techniques) 및 그 공격방식을 달성하기 위한 상세 기법(Procedures)의 TTPs 모델을 이용한 프레임워크로, 기업의 전산망 침투 관련 14개의 공격 전술정보와 193개의 공격 기술정보 및 42개의 공격 완화 정보(Mitigations)를 지원[7]한다. 또한, 모바일 및 ICS(산업제어시스템) 관련 공격 전술정보, 공격 기술정보 및 공격 완화 정보도 각각 제공[6]하고 있다. ATT&CK의 또 하나의 장점은 운영체제별(Windows, macOS, Linix), 운영환경별(Cloud, Network, Containers)로 다양한 공격기술을 분석할 수 있도록 맞춤형 분석 프레임워크를 제공한다. 따라서, 본 논문에서는 현실 세계에서 발생하는 다양한 APT 공격 분석을 분석함에 있어 사이버 킬 체인 보다 효율적이고 효과적인 ATT&CK 프레임워크를 활용한다. ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge)는 실제 사이버 공격 사례를 관찰한 후 공격자가 사용한 악의적 행위(Adversary behaviors)에 대해서 공격전술(Tactics)과 기술(Techniques)의 관점으로 분석하여 다양한 공격그룹의 공격기법을 분류해서 목록화해 놓은 표준적인 데이터의 집합[7]으로 볼 수 있다. 초창기의 ATT&CK는 MITRE에서 MS의 윈도우 운영체제를 사용하는 기업의 해킹 공격에 대해서 전술(Tactics), 기술(Techniques), 절차(Procedures) 등 TTPs를 문서화하는 것으로 시작되었으며 이후 공격자로부터 발생한 일관된 공격 행동 패턴에 대한 분석을 기반으로 TTPs 정보를 매핑하여 공격자의 행위를 식별해 줄 수 있는 프레임워크로 발전하였다. 2016년 7월 처음으로 체계적으로 정리하기 시작하였으며 2018년 1월에 정식 버전1을 공개한 이후 2023년 5월 기준으로 버전 13.1까지 지속적으로 업데이트 되고 있다.[8]

ATT&CK에서 사용하는 공격전술 14개는 <표 1>과 같으며, 각각의 목적을 달성하기 위한 공격 기술이 존재한다. 이와 같이, ATT&CK는 실제 APT 그룹의 해킹 전술 및 기법을 분석하고 도식화할 수 있으므로 공격

의 흐름 및 프로세스 관점에서 개념단계로만 기술되었던 사이버 킬 체인 모델의 약점을 보완하였다.

<표 1> ATT&CK 공격 전술 및 설명

공격전술(목적)	설명
정찰 (Reconnaissance)	대상 목표에 대한 정보수집
자원 개발 (Resource Development)	해킹을 위해 사용할 서버 등을 구축
초기 액세스 (Initial Access)	네트워크 진입을 위한 환경정보 취득
실행 (Execution)	공격자가 로컬 또는 원격 시스템을 통해 악성코드를 실행하기 위한 전술
지속 (Persistence)	공격 기반 유지 및 시스템에 지속적으로 접근하기 위한 전술
권한 상승 (Privilege Escalation)	시스템이나 네트워크에서 높은 권한을 얻기 위한 전술
방어 우회 (Defense Evasion)	공격이 탐지당하는 것을 회피하기 위한 전술
계정 접근 (Credential Access)	시스템 계정 등을 탈취하기 위한 전술
탐색 (Discovery)	시스템 및 내부 네트워크의 정보를 얻기 위한 전술
내부 확산 (Lateral Movement)	내부망으로 점거를 확산시키는데 활용하는 전술
수집 (Collection)	공격 목적 및 관련 정보가 포함된 자료를 수집하기 위해 사용하는 전술
명령 및 제어 (Command and Control)	침입한 네트워크 내부 시스템과 통신하며 제어하기 위해 사용하는 전술
탈취 (Exfiltration)	네트워크에서 정보를 탈취하기 위해 사용하는 전술
영향 (Impact)	공격 목표에 대해 가용성과 무결성을 손상, 시스템 파괴 등에 사용하는 전술

ATT&CK에서 사용하는 공격전술 14개는 <표 1>과 같으며, 각각의 목적을 달성하기 위한 공격 기술이 존재한다.

이와 같이, ATT&CK는 실제 APT 그룹의 해킹 전술 및 기법을 분석하고 도식화할 수 있으므로 공격의 흐름 및 프로세스 관점에서 개념단계로만 기술되었던 사이버 킬 체인 모델의 약점을 보완하였다.

3. MITRE ATT&CK 기반 APT 공격 분석

3.1 Kimsuky 사례

Kimsuky APT 공격조직은 2010년경부터 우리나라의 국방부와 통일부 등 정부 부처 및 유관기관을 해킹해 사회기반 시설, 탈북자 등의 관련 자료를 빼낸 북한 해킹 조직의 이름으로, 지난 2013년 러시아 정보보안업체 Kaspersky가 해커의 이메일 계정인 '김숙향(kimsukyang)'이라는 이름으로 보고서를 발표하면서 알려졌다. 이후 한국수력원자력(2014.12), 한국원자력연구원(2021.6), 서울대병원(2021.7), 한국항공우주산업, 한국핵융합연구원, 한국항공우주연구원(2021.7) 등 다양한 한국의 기관을 해킹하였다.[17]

3.2 Lazarus 사례

라자루스(Lazarus) APT 공격조직은 2009년 트로이 작전(Operation Troy)을 시작으로 지금까지 활발히 활동 중이다. 2009년부터 2014년에는 한국과 미국을 집중적으로 공격하였다. 2013년 7월 8일, 미국 보안회사 맥아피(McAfee)는 2009년부터 한국에서 발생한 트로이 작전 해킹이 한국군과 주한미군을 타깃으로 한 조직적이고 지속적인 사이버 공격 시도로 분석하였다. 트로이 작전이라고 명명된 악성 맬웨어(Malware)가 최소한 4년 이상 한국 정부와 군대의 컴퓨터들을 감염시킨 후 '미국 육군', '비밀', '키 리졸브 작전', '합참 직원' 등의 용어로 군사기밀을 검색, 수집하였다. 보고서를 작성한 맥아피 수석연구원 라이언 셔스토비토프는 "이것은 단순한 공격이 아닌 군사 간첩 행위"라고 말하였다.[18] 2015년 이후에는 금전적 수익을 목적으로 공격 범위를 넓히고 있다. 일각에서는 '히든 코브라(Hidden Cobra)'라고 부르기도 한다. 또한, 2018년 미 FBI는 라자루스 그룹 일원인 북한인 '박진혁'을 컴퓨터 사기 혐의로 기소하였다.

3.3 LAPSUS$ 사례

LAPSUS$ 해킹조직은 2021년 브라질 보건청 해킹을 시작으로 2022년에는 글로벌 기업인 Okta, Nvidia, 삼성, LG전자, T-Mobile, 마이크로소프트, 우버 등 다수의 기업을 해킹해서 수집한 다량의 정보를 판매했으며, 2022.3.24. 영국에서 7명의 조직원들이 체포되었다.

3.4 APT 그룹별 공격전술 및 기술 비교

APT 공격조직은 각 조직별로 공격전술에 활용한 방법들에 있어서 세부적으로는 다양한 차이가 있음을 확인할 수 있다. <표 2>는 ATT&CK의 14개 공격전술별로 Kimsuky, Lazarus, LAPSUS$의 특성을 분류하였다.

<표 2> APT 공격조직별 공격전술 및 기술 비교

공격전술	Kimsuky	Lazarus	LAPSUS$
정찰	이메일 주소와 이름 수집 / 이메일 계정 탈취용 피싱메일(링크) 사용 / 검색엔진(구글)과 소셜미디어(트위터)에서 공격대상 모니터링	이메일 주소 수집 / 인터넷에서 공격 대상 기관 정보수집 / 링크드인 활용	접속계정 정보 등을 다크웹 구매/코드 저장소에서 수집
자원 개발	도메인 등록 / 가상화폐와 선불카드로 호스팅 서버 구매 / 피싱메일 발송용 이메일 계정 확보 / 악성코드 유포를 위한 블로그 개설 / 악성코드 자체 개발 / WebBrowserPassView, Mimikatz 등사용	도메인 등록 / 호스팅 서버 구매 / 악성코드 개발 / 스피어피싱용 이메일 가입 / 링크트인 및 트위터 계정 개설 /코드 사인용 인증서 사용, Putty PSCP, ChromePass 등 도구 사용	Virtual Private Server 이용/비밀번호 스틸러 사용
초기 액세스	피싱메일(첨부파일, 링크) / 피싱을 통해 수집한 유효한 관리자 계정 사용	MS Exchange 공격도구 개발 / RDP / 피싱메일(첨부파일, 링크) / GREASE 툴을 이용해서 RDP에 관리자 계정 추가	VPN, RDP 등 접속 / 클라우드 계정을 이용
실행	자바스크립트를 이용해서 로컬그룹에 사용자 추가 / 파워쉘, 파이썬, 비주얼베이직, 윈도우 커맨드명령어 사용 /WebBrowserPassView로 계정정보 수집	파워쉘을 이용해서 악성코드 및 명령어 실행 / MS워드에 VBA스크립트를 삽입, 악성코드 전파 / WMIC를 이용해서 내부 확산(Lateral Movement)	기업 내부 사용자의 PC에 원격관리 툴 설치
지속	레지스트리에 악성코드 실행 등록 / 로컬에 사용자 계정 추가 / 악성코드 윈도우서비스로 등록 / RDP 사용 및 관리자 계정 추가	WhiskeyDelta2를 활용, 관리자 계정 이름 변경 / 시작 폴더 레지스트리에 악성코드 실행 등록 / 악성코드 윈도우 서비스로 등록 등	클라우드 인스턴스에 Global 관리자 추가
권한 상승	프로세스 인젝션 / GREASE 툴을 이용해서 관리자 계정 추가	키로거(KiloAlfa)로 토큰 입수 및 프로세스 생성 / DLL Injection	패치가 안된 Jira, GitLab, Confluence 취약점 악용
방어 우회	BASE64를 이용해서 VBScript 난독화 / 포렌식 방해를 위해 파일 생성 타임스탬프 조작 / UPX로 실행파일 난독화 / 정상 인증서로 악성코드에 전자 서명	파일 난독화 / 파일 속성(Hidden, System) 변경 / 윈도우 디펜더 및 방화벽 비활성화 / Themida를 이용해서 DLL 파일 등 난독화 / 코드 서명	유효한 클라우드 계정/클라우드에 신규 가상머신 설치
계정 접근	PHProxy 툴을 이용한 웹 트래픽 가로채기 / 크롬 브라우저 저장 비밀번호 및 쿠키 탈취 / 키 로깅	SMB 취약점 공격 / 취약한 비밀번호 대입 공격 / 키로거 사용	웹 브라우저 저장 비밀번호 탈취 /네트워크탈취 세션토큰 재사용, MFA 무력화/AD 공격
탐색	파일 및 디렉토리 탐색 / 네트워크 스니핑(계정정보 획득) / 프로세스 및 레지스트리, 백신프로그램, 시스템 정보, 네트워크 정보 탐색	Active Directory 서버 정보 수집 / 파일 및 디렉토리 수집 / 네트워크 정보 수집 등	도메인 계정/도메인 그룹
내부 확산	내부 사용자에게 피싱메일 유포 / RDP 이용 /Command&Control 서버 접속에 Pass the Hash 기법 사용	내부 사용자에게 피싱메일 유포 / RDP 이용 / SMB 이용 / 터널링에 SSH 및 PuTTy SCP 사용	N/A
수집	PHProxy 툴을 이용한 웹 트래픽 가로채기 / 탈취 문서를 RC4로 암호화 및 QuickZip으로 압축 / 오피스, PDF, HWP 문서 검색 및 수집 / 피해자 이메일에 자동 포워딩 기능 세팅 / 윈도우 파워쉘 기반의 키로거 MECHANICAL을 통해 키 로깅	탈취 문서를 XOR로 암호화 및 Zlib로 압축 전송 / 키로깅 정보	코드저장소 /Confluence/ Sharepoint/E mail-Forwarding
명령 및 제어	추가 악성코드 다운로드를 위해 FTP 프로토콜 이용 / C2 서버와 통신시 웹 기반의 HTTP GET, POST Method 사용 / TeamViewer를 개조해서 C2 서버와 통신	C2 서버와 통신에 HTTP 및 HTTPS 사용 / Base64 인코딩 / XOR 또는 AES 암호화 사용 / 악성코드에 하드코딩된 C2 서버에 접속해서 데이터 전송	NordVPN 사용
탈취	C2 채널을 통해 데이터 탈취 / 탈취한 데이터는 Blogspot에 저장	C2 채널을 통해 데이터 탈취 / 탈취한 데이터는 Dropbox에 저장	N/A
영향	N/A	데이터 파괴 / 디스크 삭제 / 서비스 중지 / 시스템 셧다운	Global Admin 계정삭제/데이터 파괴

4. 산업기술 유출방지를 위한 보안 프레임워크

4.1 APT 공격 대응을 위한 보안 요구사항

각 공격전술별 해킹조직의 공격 방법을 분석해서

<표 3>과 같이 보안 요구사항 26개를 도출하였다. 도출한 보안 요구사항은 시스템으로 구현 가능한 기술적(Technical, T로 표시) 방안 외에도 직원 인식 교육 등의 관리적(Administritive, A로 표시) 방안 및 물리적(Physical, P로 표시) 방안도 함께 고려하였다.

보안 요구사항을 도출할 때 효율적이고 효과적인 보안 대책을 수립하기 위해서는 기술적, 관리적 보안방안 외에도 물리적인 보안방안을 동시에 고려하여야 한다. 물리적 보안대책을 고려해야 하는 이유는 다음과 같다. 공급망(Supply Chain) 보안 관련해서 APT 공격조직은 타깃 기업에 직접적인 침투가 어려운 경우에 타깃 기업에 소프트웨어를 공급하거나 유지보수를 담당하는 외부 업체를 해킹 한 후 경유지로 악용해서 목표하고 있는 타킷 기업에 접근하는 경우이다. 주로, 유지보수에 활용하는 노트북이나 USB 메모리 장치에 악성코드를 은닉시킨 후 타깃 기업의 PC 또는 서버 등의 자산에 연결할 경우 악성코드에 감염시키는 기법을 악용한다. 이에 대한 대표적인 사례로는 2011년 농협 전산망 해킹사고가 있다. 2011년 4월 12일 농협 서버 587대 중 273대가 피해를 입은 초대형 금융사고로 APT 공격조직은 7개월 동안 유지보수 업체(IBM) 직원의 노트북을 감시하고 있다가 농협 전산망에 연결되는 순간 서버 삭제 명령어를 전송하는 방법을 사용하였다.[12] 따라서, 이러한 유형의 APT 공격을 방어하기 위해서는 유지보수 목적으로 반입하는 내외부 직원의 USB나 노트북에 대한 반입 통제 및 반입 전에 악성코드를 검사하고, 스마트폰 테더링, LTE 라우터 등의 인터넷 연결이 가능한 통신장비 반입여부 등을 점검하는 물리적인 절차도 추가 및 강화해야 한다. 본 논문에서는 관리적 방안 3개(SR-3, 19, 25), 물리적 방안 3개(SR-6, 8, 10) 및 기술적 방안 20개(SR-1, 2, 4, 5, 7, 9, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 26) 등 총 26개의 보안요구사항을 도출하였다.

<표 3> 공격전술별 보안요구사항 분석

공격전술 (목적)	보안 요구 사항(Security Requirements, SR)		기술적(T) 관리적(A) 물리적(P)
	번호	내용	
정찰 (Reconnaissance)	SR-1	o 공개 사이트 등에 정보 노출여부 주기적 확인 시스템 구축	T
자원 개발 (Resource Development)	SR-2	o 악성 도메인 블랙리스트 관리 시스템 개발	T
	SR-3	o 회사 차원의 캠페인 전개(웹 브라우저에 로그인 비밀번호 저장 금지 등)	A
초기 액세스 (Initial Access)	SR-4	o 피싱메일 탐지 수단 강구	T
	SR-5	o 원격접속프로그램 접근통제	T
	SR-6	o 노트북 반입 절차 및 통제 수단 마련	P
	SR-7	o 악성코드 검사 시스템 구축	T
	SR-8	o USB 반입 절차 및 통제 수단 마련	P
	SR-9	o 악성코드 검사용 시스템 구축	T
	SR-10	o 내외부 직원의 스마트폰 테더링 등 장비 반입 통제	P
	SR-11	o 무선 테더링 차단시스템 구축	T
실행 (Execution)	SR-12	o 시스템 관련 명령어 실행 차단	T
	SR-13	o Powershell 등 실행 차단	T
지속 (Persistence)	SR-14	o 레지스트리 접근 명령어 차단	T
권한 상승 (Privilege Escalation)	SR-15	o 취약점 패치 관리	T
방어 우회 (Defense Evasion)	SR-16	o 윈도우 기본 실행파일 접근 통제	T
계정 접근 (Credential Access)	SR-17	o 시스템 도입시 기본적으로 설정되어 있는 기본 비밀번호 변경	T
	SR-18	o 비밀번호 설정 정책 도입(특수문자 포함 9자리 이상)	T
	SR-19	o 회사 차원의 캠페인 전개(웹 브라우저에 로그인 비밀번호 저장 금지 등)	A
탐색 (Discovery)	SR-20	o Active Directory 관련 정보 수집 명령어 차단	T
내부 확산 (Lateral Movement)	SR-21	o 피싱 메일 차단시스템 도입	T
수집 (Collection)	SR-22	o 이메일 시스템에서 메일 포워딩 여부 주기적 확인	T
명령 및 제어 (C&C)	SR-23	o C2C 서버로 악용된 블랙리스트 서버 관리	T
탈취 (Exfiltration)	SR-24	o C2C 서버로 악용된 블랙리스트 서버 관리	T
영향 (Impact)	SR-25	o 백업 및 복구 절차 마련	A
	SR-26	o 백업 및 복구 시스템 구축	T

4.2 산업기밀 유출 방지를 위한 보안 프레임워크

APT 공격조직의 공격 행태 분석을 통해 보안 요구사항 26개를 도출하였으며, 이를 기반으로 보안 프레임워크를 제안하고자 한다. 보안 프레임워크를 구현함에 있어, 기술적인 방안 외에도 직원 보안 교육 등의 관리적 방안 및 물리적 방안도 함께 고려하여야 한다. 관리적, 물리적, 기술적 강화방안을 적용한 보안 프레임워크는 (그림 1)과 같다.

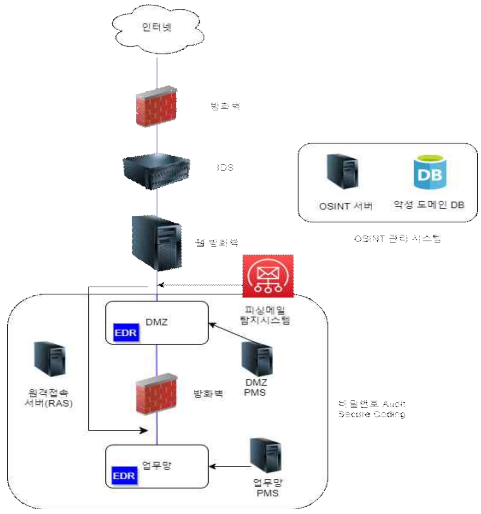
분야	ATT&CK 공격 전술(14개)														
	정찰	자원발	초기액세스	실행	지속	권한상승	방어우회	계정접근	탐색	내부확산	수집	명령제어	탈취	영향
관리		SR-3						SR-19						SR-25
물리		SR-6												
		SR-8												
		SR-10												
기술	SR-1	SR-2	SR-4	SR-12	SR-14	SR-15	SR-16	SR-17	SR-20	SR-21	SR-22	SR-23	SR-24	SR-26
			SR-5	SR-13				SR-18						
			SR-7											
			SR-9											
			SR-11											

(그림 1) 보안 프레임워크

4.3 보안 아키텍처 구현 방안

앞에서 살펴본 보안 요구사항을 충족시키기 위한 시스템이나 솔루션은 기존에 기업에서 보유하고 있는 경우도 있다. 따라서, 신규 시스템을 도입 또는 구축시 회사 보유 시스템과 연동 가능하도록 구현하여야 한다.

(그림 2)와 같이 TO-BE 아키텍처 구현에 사용되는 관련 시스템을 살펴보면 다음과 같다. 첫 번째로, 보안에 취약한 원격접속(Telnet, RDP, VNC, Teamviewer 등)을 대체할 원격접속 서버(Remote Access Server)를 도입한다. RAS는 내외부에서의 모든 원격 접속은 RAS를 통해서만 접속하도록 접속지점을 단일화하여, 사용자의 행위를 실시간 모니터링하고 이상징후 발견시 세션을 차단하는 등의 Active한 보안정책을 적용해야 한다.



(그림 2) TO-BE 아키텍처 구성도

두 번째로, 피싱메일에 효과적으로 대응하기 위해 이메일의 모든 내용을 텍스트로 변환해서 사용자에게 전송해 줌으로써 피싱 URL을 클릭할 수 없도록 원천 봉쇄하는 시스템을 구축 또는 적용하여야 한다.

세 번째로, 다크웹 및 인터넷에서 유통되는 기업의 정보를 실시간으로 모니터링할 수 있는 OSINT(Open Source Intelligence) 관리시스템을 구축하는 것이다. OSINT 관리시스템에서는 주기적(매일 또는 시간 단위)으로 OSINT 사이트에 접속해서 회사의 중요 정보(시스템 접속 정보, 사용자 계정 정보 등)가 유통되고 있는지를 집중 모니터링한다. 네 번째로, 회사의 모든 시스템의 소스코드는 Secure Coding 진단 S/W를 활용해서 취약점을 진단하고, 비밀번호를 주기적으로 점검해서 유추하기 쉬운PW는 변경하도록 하는 등의 적극적인 보안활동을 전개하는 것이다. 또한, DMZ 서버 및 내부망PC 등에 악성코드를 탐지하고 차단하는 EDR(Endpoint Detection & Response)을 설치하는 것이다.

5. 결론

지능형 지속위협(APT) 공격조직들은 산업기밀을 보유한 기업이나 기관을 해킹, 국가적으로 중요한 산업기밀을

탈취해서 제3국에 판매하거나 기술격차를 줄이는데 활용하므로, APT 공격조직에 대한 방어체계 구축은 국가안보 차원에서 접근이 필요하다. 그러나, 방어자 입장에서 고도화된 공격을 모두 방어하기에는 분명한 한계점이 존재한다. 이러한 한계점을 극복하기 위해 본 논문에서는 우리나라를 대상으로 APT 공격을 감행한 3가지 조직의 공격 수법을 ATT&CK 툴로 분석하였다.

조직별로 공격 유형 및 공격방법을 교차 분석하였으며, 그에 따른 방어자 입장에서의 보안 요구사항(SR, Security Requirements) 26개를 도출하였다. 도출된 보안요구사항은 관리적, 물리적, 기술적 방안으로 구분해서 보안대책을 수립할 수 있다.

또한, 각 보안 요구사항 별로 보안대책을 매핑하는 보안프레임워크를 제안하였고, 이를 기반으로 APT 공격에 효과적으로 대응하기 위한 신규 시스템 도입 또는 구축방안도 제안하였다. 본 논문은 보안시스템 개발 및 운영자들이 기업의 산업기밀 유출 방지를 위한 보안업무에 실질적으로 활용할 수 있도록 현재의 기술로 구현 가능한 시스템으로 구성하였다. 한편, 본 논문에서 도출한 보안요구사항, 보안프레임워크 및 시스템 구축 방안이 APT 공격을 방어하는 절대적인 방법이 될 수는 없으나, APT 공격조직의 공격 행태는 유사한 방법으로 진행된다는 점에 착안해서 주기적으로 공격 방법 등을 분석해서 모듈 형태로 본 프레임워크에 추가 한다면 각종 해킹 공격에 효과적으로 대응할 수 있다고 생각한다.

향후, 이 논문을 기반으로 각종 사고사례를 통해 실체가 파악된 다양한 APT 공격조직의 고도화·지능화된 공격을 ATT&CK 툴로 분석해서 보안 요구사항을 도출 한 후 보안대책을 마련하는 추가적인 연구가 필요하다.

참고문헌

[1] LockheedMartin, “Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform”, lockheedmartin.com, 2015.

[2] Eric M. Hutchins, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, www.lockheedmartin.com, 2011.

[3] 윤영인, 김종화, 이재연, 유석대, 이상진, “APT 공격 사례 분석을 통한 사이버 킬체인과 TTP에 대한 연구”, 융합보안논문지, 제20권, 제4호, pp92-99, 2020.

[4] Jung-Sik Lee, Sung-Young Cho, Haeng-Rok Oh, Myung-Mook Han, “A Study on Defense and Attack Model for Cyber Command Control System based Cyber Kill Chain”, Journal of Internet Computing and Services(JICS), pp.41-50, 2021.

[5] 안명길, 이정륜, “사이버 전투실험 분석을 위한 MITRE ATT&CK 기반의 시스템 구성 및 방법론 연구”, 한국컴퓨터정보학회논문지, vol.25, no.7, 통권197호, pp.31-37, 2020.

[6] 안광현, 오재헌, 여서래, 박원형, “MITRE ATT&CK 기반 산업기술유출 방지 프레임워크 기술”, 정보보호학회지, Vol. 21, Issue 3, pp.29-38, 2021.

[7] MITRE, https://attack.mitre.org/.

[8] https://github.com/mitre/cti/releases/.

[9] Kimsuky, https://attack.mitre.org/groups/G0094/.

[10] Lazarus, https://attack.mitre.org/groups/G0032/.

[11] LAPSUS$, https://attack.mitre.org/groups/G1004/.

[12] 전성철, “검찰 농협 해킹, 北 정찰총국이 7개월간 준비”, 동아일보, 2011년 5월 4일.

[13] 서지민, “KAI, 해킹 수사 의뢰...‘K-2’ 설계도면 유출 가능성”, 시사저널, 2021년 6월 30일.

[14] 오수진, “북 해커조직 '김수키' 블랙리스트 올랐다… 위성·군사기밀 해킹”, 연합뉴스, 2023년 6월 2일.

[15] 김영명, “민·관·학, ‘산업기밀 탈취 해킹’ 공동 대응방안 마련한다”, 보안뉴스, 2022년 12월 15일.

[16] 장용석, “원자력硏 12일간 해킹 노출…대우조선해양 '암호화폐' 협박까지”, 뉴스1, 2021년 7월 8일.

[17] 박형주, “한국 방산 기관 '북한 해커'에 잇따라 뚫려… "한국 군사·기술력 파악 시도"”, VOA, 2021년 7월 9일.

[18] 정의식, 美보안회사 ‘맥아피’,“2009년부터 한국 해킹한 세력 포착”, CNBNews, 2013년 7월 9일.

〔저자소개〕

임 양 규 (YangKyu Lim)

1999년 2월 국민대학교 학사
2002년 2월 성균관대학교 석사
2022년 2월 단국대학교 박사과정 수료
email : jasonlim@dankook.ac.kr

박 원 형 (WonHyung Park)

2002년 서울과학기술대학교 산업정보시스템공학과 공학사
2006년 서울과학기술대학교 정보산업공학과 공학석사
2009년 경기대학교 정보보호학과 이학박사
2015년 성균관대학교 컴퓨터교육학과 박사수료
2020년 ~ 2022년 상명대학교 정보보안공학과 교수
2023년 3월 ~ 현재 성신여자대학교 융합보안공학과 교수
email : whpark@sungshin.ac.kr

이 환 수 (HwanSoo Lee)

2003년 2월 단국대학교 학사
2005년 2월 연세대학교 석사
2014년 2월 한국과학기술원 박사
현재 단국대학교 산업보안학과 교수
email : hanslee992@gmail.com