정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

MITRE ATT&CK 기반 산업기술유출 방지 프레임워크 기술

안 광 현*, 오 재 헌**, 여 서 래***, 박 원 형****

요 약

산업안보위협은 개인 또는 전·현직자의 이익을 위해 다양한 경로를 통해 지속적으로 산업기술들을 유출하였지만, 최근에는 국가에서 지원하는 사이버 공격자 그룹을 활용하여 신기술을 탈취하려는 목적의 사이버공격을 감행하고 있어 현재 산업체뿐만 아니라, 국가경제의 손실이 매우 크다. 따라서 본 논문에서는 정보탈취를 목적으로 하는 국가 배후 해킹조직의 침투 경로 및 공격 단계와 국가핵심기술 유출 사례와 연계하여 MITRE社 ATT&CK 프레임워크를 활용하여 산업기술위협에 대응할 수 있는 기술을 소개 한다.

Ⅰ. 서 론

최근 산업안보위협이 고도화됨에 따라 개인 또는 전·현직의 이익을 위해 산업기술들을 유출하는 반면 현재는 범국가적으로 타국가의 신기술을 탈취하려는 목적의 사이버공격자 그룹을 지원하여 사이버공격을 감행하고 있어 정보유출에 대응할 수 있는 방안에 대한 중요성이 대두되고 있다[1].

국가정보원 산업기밀보호센터의 국정감사 자료에 의하면, 年 평균 산업기술유출을 피해를 받은 산업체의 예상 피해 금액은 한화 약 50조 원으로 이러한 결과는 중소기업 4,700여개의 연 매출과 맞먹는 금액으로 분석되고 있다[2].

하지만, 산업기술유출 방법은 더욱 지능화되어 주요국가 및 해외 기업들과의 치열한 경쟁관계인 국내기업의 국가핵심기술들을 대상으로 사이버공격자 그룹을 활용하여 수단과 방법을 가리지 않고 탈취하려는 목적으로 지속 시도하고 있으며 산업기술위협을 효율적으로 대응할 수 있는 방안이 부족한 실정이다. 이러한 현실로 인하여 국가의 안전보장과 국민경제 발전에 중대한 악영향을 미치고 있다[2].

따라서 본 논문은 국가핵심기술 유출 사례를 바탕으로 정보탈취를 목적으로 하는 국가 배후 해킹조직의 침투 경로 및 공격 단계와 연계시켜 MITRE ATT&CK 프레임워크 기반의 산업기술위협을 대응할 수 있는 방안을 제안한다.

Ⅱ. 관련 연구

2.1. MITRE社 ATT&CK 프레임워크 분석

ATT&CK(Adversary Tactics and Techniques, Common Knowledge)는 MITRE社에서 제공하는 표준 프레임워크로 네트워크 내에 활동하는 공격자의 실제 행위를 기반으로 전술, 기술, 절차, 사용한 공격소프트웨어 등 사이버 킬체인 7단계를 14단계로 폭 넓은 공격 프로세스로 포맷한 프레임워크이다[6]. ATT&CK 기반의 공격자 전술단계 및 전략 패턴은 [표 1]과 같다.

* 세종대학교 컴퓨터공학과 석·박사통합과정 (대학원생, rhkdgus8781@sju.ac.kr)
** 딜로이트 안진회계법인 (컨설턴트, jaehoh@delotte.com)
*** 코리아서버호스팅(주) 보안관제팀 (매니저, ysr@iteasy.co.kr)
**** 상명대학교 정보보안공학과(부교수, whpark@smu.ac.kr)

〔표 1〕 ATT&CK 기반 공격자 전술, 전략 패턴

Tactic ID	Tactic	Explanation
TA0043	Recon	Gather information that can be used to plan future operations
TA0042	Resource Development	Attackers build resources they can use to support their operations.
TA0001	Initial Access	Intrude the network
TA0002	Execution	run malicious code
TA0003	Persistence	Attackers continue to attempt attacks to succeed in their operations.
TA0004	Privilege Escalation	Attackers steal top-level privileges
TA0005	Defense Evasion	Attackers bypass information protection systems
TA0006	Credential Access	Attacker to steal account name and password
TA0007	Discovery	Exploring the vulnerable environment of the target
TA0008	Lateral Movement	Attempt to infiltrate the target's environment
TA0009	Collection	Attackers gather information tailored to their targets.
TA0011	C&C	Attackers communicate with compromised systems to control
TA0010	Exfiltration	Data leakage
TA0040	Impact	Attackers manipulate and destroy systems and data.

2.2. 국가핵심기술 현황 분석

산업기술의 유출방지 및 보호에 관한 법률 제9조(국가핵심기술의 지정 · 변경 및 해제 등)에 따라 지정된 국가핵심산업기술 현황은 [표 2] [표 3]과 같다[8].

〔표 2〕 국가핵심기술 총계 현황

Div	Semiconductor	Display	Electrical Electronics	Machine	Robot	Space
	10	2	3	7	3	4
Div	Steel	Car/ Railway	Ship building	Nu-clear	I&C	Bio
	9	9	8	5	7	4
합계 : 71						

〔표 3〕 국가핵심기술 현황 분석

Division	Explanation
Semiconductor (10)	- Design, process, electromagnetism, and three-dimensional stacking technology corresponding to 30 nano-class DRAMs. - Additive assembly technology and inspection technology corresponding to DRAM - Design, process, and device technologies that are equivalent to 30-nano or stacked 3D NAND-Flash - Additive assembly technology and inspection technology corresponding to NAND flash - Process/electromechanical technology and three-dimensional stacking technology corresponding to 30-nano-class or lower foundry - Mobile Application Processor SoC Design and Process Technology - LTE/LTE_adv/5G Baseband Modem Design Technology - Single-crystal growth technology for manufacturing large diameter (300mm or higher) semiconductor wafers - Design, process, and electronic technology of image sensors that are less than 1μm pixel - Technology for assembling and inspecting advanced packages (FO-WLP, FO-PLP, FO-PoP, etc.) for system semiconductors
Display (2)	- Design, process, and manufacturing of TFT-LCD panels with 8th generation level (2200x2500 mm) or higher (excluding module assembly process technology) and operation technology - Design, process, and manufacturing of AMOLED panels (excluding module assembly process technology)
Electrical Electronics (3)	- Medium and large high energy densities such as electric vehicles (pouch-type 265Wh/kg or more or square-type 90% pouch-type) Lithium secondary battery design, process, manufacturing and evaluation technology - Lithium secondary battery Ni content exceeding 80% Anode material design, manufacturing and process technology - Design and manufacturing technology for power cable systems over 500kV (including connections)

Robot (3)	- Design Technology and Manufacturing Technology of Laparoscopic, Endoscopic and Image-Induced Surgical Robot Systems - Robotic operation and control technologies for dense process tasks that share workspaces - Video surveillance based robot integrated control technology
Space (4)	- High performance cryopump technology - Cryogenic/High Pressure Diaphragm Drive Opening/Closing Valve Technology - Ultra-high resolution (50 cm based on altitude 500 Km) optical satellite high speed maneuver precision posture control meter design technology - Technology for assembling, aligning, and inspecting electronic optical cameras mounted with a diameter of at least 1m;
Machine (7)	- Design and Manufacturing Technologies for Multi-Axis Multi-Processing Turning Centers - Design and manufacturing technologies for high precision 5-axis machining centers - Medium to large excavator reliability design and manufacturing technology - Design of diesel engines and post-processing systems to meet Tier 4F emission regulations for Off-road - Load-sensitive hydraulic transmission design and manufacturing technology for tractors - Low GWP Refrigerant Response High Efficiency Turbo Compressor Technology - Technology for designing and operating a human-friendly elevator system with low vibration, low noise, and dynamic stability;
Biotechnology (4)	- Large-scale fermentation refining technology for antibodies (animal cell culture/refinery process technology of 10,000 liters or more) - Botulinum toxin production technology (including strains that produce botulinum toxin) - Atomic microscope manufacturing technology (True non-contact mode technology, Narrow Trench measurement technology, 3D analysis technology for semiconductor devices of 30 nm or less, nano measurement technology for samples with a large area of 300 mm or more, SPM fusion technology)
	- Multi-type immune analysis system technology for infectious diseases using biomarker immobilization technology (more than 3 types, sensitivity and specificity of 95% or more)
Steel (9)	- FINEX flow furnace operation technology - Technology for manufacturing rebar/shape steel with yield strength of 600MPa or higher [Low carbon steel (0.4% C or less)] - Manufacturing technology of TWIP steel with high-grade manganese (10% Mn or more) - Giga-class high-strength steel sheet manufacturing technology with less than 4% of the total amount of alloying elements - Manufacturing technology for shipbuilding and power plants 100 tons or more (based on single product) large-sized liquor and single steel manufacturing technology - Low Nickel (3% Ni or less) High Nitrogen (0.4% N or more) Stainless Steel Manufacturing technology - Al-based ultra-precision plating (resolution 0.1μm) control technology - Automatic control technology for furnace operation based on deep learning artificial intelligence - High strength steel plates with a tensile strength of 600MPa or higher Smart water cooling technology for manufacturing (including engineering and control technologies)
Car/ Railway (9)	- Gasoline Direct Injection (GDI) Fuel Injection System Design and Manufacturing Technology - Hybrid and power-based automotive (xEV) system design and manufacturing technologies (Control Unit, Battery Management System, Regenerative Braking System only) - Design, process, and manufacturing technology of hydrogen electric vehicle fuel cell system (hydrogen storage, supply, stack and BOP) - LPG Direct Injection (LPDi) Fuel Injection System Design and Manufacturing Technology) - Design and manufacturing technologies for diesel engine fuel injection devices, super-systems and exhaust post-processing units above Euro 6 (DPF, SCR only)

	- Design and manufacturing technology for automotive engines and automatic transmission (Provided, That technology is limited to within two years after mass production) - Body Design and Manufacturing Technology for All-in-One Railway Vehicles Using Multi-Materials - Design and manufacturing technologies for high-speed train power systems with speeds greater than 350 km/h (AC induction motor, TDCS control diagnosis, and main power converter technology only) - Design and manufacturing technologies for core parts and systems of autonomous vehicles (limited to camera systems, radar systems, rider systems, and precision location detection systems)
Shipbuilding (8)	- High value-added ships (large container ship, low temperature liquefaction tank ship, large cruise ship, glacial cargo ship) design technology for gas fuel propulsion ships, electric propulsion ships, etc.) and marine systems (sea structures, marine plants, etc.; - Liquefied gas cargo hold, fuel tank design and manufacturing technology - Construction technology of ship and marine structures on land and on-board blocks for ships and marine structures of more than 3,000 tons; - Manufacturing technology for diesel engines with more than 5,000 horsepower, crankshafts, and propellers with a diameter of more than 5m - Technology of autonomous operation (economic operation, safe operation, etc.) and navigation automation, and integrated control system for ships; - ERP/PLM System and CAD-Based Design and Production Support Program for Shipbuilding - Core equipment manufacturing technology for ships (BWMS manufacturing technology, WHRS manufacturing technology, SCR and EGCS, etc.)) - Manufacturing technology, such as fuel supply, re-liquefaction, and re-ventilation systems for gas fuel propulsion ships;
Nuclear (5)	- Nuclear power plant passive auxiliary water supply system technology - Remote visual inspection technology on the secondary side of the nuclear power plant steam generator. - Neutron Mirror and Neutron Guide Tube Development Technology - Research reactor U-Mo alloy nuclear fuel manufacturing technology - New light water reactor power control system technology
Information and Communication (7)	- LTE/LTE_adv System Design Technology - PA design technology that minimizes base station miniaturization and power - LTE/LTE_adv/5G Measuring Device Design Technology - Giga-class mobile backhaul technology for ultra-fast data transfer and reception - Key technologies for optical communication for software-defined network (SDN) implementation - Quantum repeater technology based on quantum theory for application of communication equipment - Design Technology for 5G Systems (Beamforming/MIMO and Mobile Network)

2.3. 산업기술탈취형 사이버공격자 그룹 프로파일링

산업기술 탈취형 사이버공격자 그룹의 현황 분석은 [표 4]과 같다[4][5].

〔표 4〕 산업기술탈취형 주요 해커조직 프로파일링 결과표

Organization	Target	Explanation
Chimera	Steal Information Spy	China's behind cyber threat group is conducting cyberattacks on semiconductors and aviation
Ajax	Spy	Iran's cyber threat group distributes malicious code to defense, electronics, etc.
admin@338	Finance, Economy and Trade, Electronics	China's behind-the-scenes cyber threat groups attack mainly on RAT and backdoor

APT17	Semiconductor, Shipbuilding, Information Technology	China's behind-the-scenes cyber threat group attempts to break into networks targeting defense, trade, aviation and information technology
APT19	Telecommunications, nuclear power, finance.	China's behind-the-scenes cyber threat groups conduct targeted attacks on a variety of industries including defense, finance, nuclear power, information and communications, high-tech, etc.
Bronze Butler	Government, biotechnology, electronics, chemistry.	Cyber spy group behind China conducts cyberattacks on biotechnology, electronics, and chemistry

2.4. 연도별 주요 산업기술 유출 현황 분석

국가정보원 산업기밀보호센터에서 조사한 연도별 주요 국가핵심 산업기술 유출 현황 분석은 [표 5]과 같다.

〔표 5〕 국가핵심 산업기술 유출 사례 분석

Year	Field	Cases
2018	Electrical and Electronics	Established a similar company in cooperation with China by retiring after leaking OLED-related equipment technical drawings without permission
2018	Environment	Prevention of air pollution, technology design, and operation data using personal storage media, and unauthorized leakage and sale to China;
2017	Ship building	Establishment of the same industry after an unauthorized leak to Malaysia, such as a special flight ship design and calculation formula;
2016	Ship building	Unauthorized spill to India, such as LNG carrier fuel supply design technology
2015	Machine	Unauthorized leakage of vehicle transmission inspection equipment technology to China through personal external hard drives, etc.

2.5. 산업기술 유출 환경 분석 및 주요 방법

본 장은 경찰대학 치안정책연구소에서 발표한 산업기술 유출경로 연구 자료로 산업기술 유출 경로 분석하여 정리한 것이다. 산업기술 유출 환경 분석 및 주요 방법 내용은 크게 1) 내부유출, 2) 외부유출, 3) 내부유출 방법, 4) 외부 유출 방법 5) 산업기술 유출대상자, 6) 유출 방법을 [표 6]에서 분류하였다[9].

〔표 6〕 산업기술 유출 경로 분석

Division	Type	Content
1	Internal Exfiltration	Former and current employees, internal employees, public offering with the company to be relocated, transfer to the same affiliate, outflow to management negligence, scouting of competitors, foreign researchers, start-up of the same business
2	External Exfiltration	Participants in technology development such as intercompany M&A, mergers and acquisitions, joint research, subcontractors, and suppliers
3	Internal Exfiltration Method	Mobile storage media such as mobile phone, USB, external hard drive, Internet e-mail, web hard drive, business computer hard disk replacement, Internet cloud, digital camera, foreign server use

4	External Exfiltration Method	Cyber leaks such as hacking, industrial espionage, Instagram, Facebook, etc.
5	Exfiltration target	Employees, former employees, retirees, partners, M&A, academic professionals.
6	Key Exfiltration Methods	hacking, mobile storage, smartphone, internet, hard copy, photography

Ⅲ. MITRE ATT&CK 기반 기술

3.1. 주요 해커조직이 활용한 ATT&CK 기반의 공격 전술 및 소프트웨어 분석

본 장에서는 2.3. 산업기술탈취형 사이버 공격자 그룹 프로파일링과 연계하여 ATT&CK 기반으로 적용한 주요 해커조직이 사용한 전술과 기법, 소프트웨어 등 공격 활동 분석 결과이다.

3.1.1. Chimera 해커조직이 활용한 ATT&CK 기반의 공격 전술 및 소프트웨어

Chimera 해커조직이 활용한 ATT&CK 기반의 공격 전술, 기법 및 소프트웨어 데이터를 구분 및 분석한 결과는 [표 7]과 같다[10].

〔표 7〕 ATT&CK 데이터 기반의 Chimera 해커조직의 국가핵심기술 탈취 목적의 공격전술 및 공격기법 분석 (일부)

Tactic	Technology	Explanation
TA0007	Account Navigation	Search domain accounts including administrator accounts as net user /dom or net user administrator
TA00011	Application Layer Protocol Exploitation	Hackers leverage the Cobalt Strike attack tool to encapsulate C2 in DNS traffic
TA0009	Archive collected data	Use a custom DLL to continuously retrieve data from memory
TA0007	Browser Bookmark Navigation	type \\c$\Users\Favorites\Links\Bookmarks bar\Imported From IE*citrix* command
TA0006	Brute Force	Use credential stuffing for victim's remote service to obtain a valid account
TA0002	Command & Script Interprinter	Run malicious payloads using PowerShell scripts and use DSInternals PowerShell modules to enable Active Directory features
TA0010	Outflows through C&C channels	Using the Cobalt Strike C2 Beacon for Data Leak
TA0001 TA0003	Utilize external remote services	Log in to external VPN, Citrix, SSH, and other remote services using a legitimate account
TA0007	Navigating files and directories	Use multiple commands to identify data of interest in file and directory lists
TA0005	Maskerading	Rename the malware to GoogleUpdate.exe and WinRAR to jucheck.exe, Recorded TV.ms, teredo.tmp, update.exe and msadcs1.exe.

3.1.2. Ajax 해커조직이 활용한 ATT&CK 기반의 공격 전술 및 소프트웨어

Ajax 해커조직이 활용한 ATT&CK 기반의 공격 전술, 기법 및 소프트웨어 데이터를 구분 및 분석한 결과는 [표 8]과 같다[11].

〔표 8〕 ATT&CK 데이터 기반의 Ajax 해커조직의 국가핵심기술 탈취 목적의 공격전술 및 공격기법 분석(일부)

Tactic	Technology	Explanation
TA0006	Obtain account permissions for the password store	Using FireMalv customized development malicious code that collects passwords from the Firefox browser repository
TA00011	Ingress Tool Transfer	Use Wrapper / Gholee, a customized development malware that downloads additional malware to infected systems
TA0001	Spear Phishing	Use a spear phishing attachment
TA0002	User Execution: Malicious Files	Run malicious files by enticing targets

3.1.3. admin@338 해커조직이 활용한 ATT&CK 기반의 공격 전술 및 소프트웨어

admin@338 해커조직이 활용한 ATT&CK 기반의 공격 전술, 기법 및 소프트웨어 데이터를 구분 및 분석한 결과는 [표 9]과 같다[12].

〔표 9〕 ATT&CK 데이터 기반의 admin@338 해커조직의 국가핵심기술 탈취 목적의 공격전술 및 공격기법 분석(일부)

Tactic	Technology	Explanation
TA0005	Maskerading	Rename the malware to GoogleUpdate.exe and WinRAR to jucheck.exe, Recorded TV.ms, teredo.tmp, update.exe and msadcs1.exe.
TA0007	Navigating files and directories	Use multiple commands to identify data of interest in file and directory lists
TA0007	Exploring System Network Configuration	Attackers use ipconfig /all 〉〉 %temp%\download command after exploiting a system with LOWBALL malware to obtain information about the OS.
TA0007	Explore system network connections	Attackers use the netstat -ano 〉〉 %temp%\download command after exploiting a computer with LOWBALL malware to display network connectivity
TA0007	System service discovery	Angreifer verwenden den Befehl net start 〉〉% temp% \ download, nachdem sie das System mit LOWBALL-Malware ausgenutzt haben, um Informationen zum Dienst zu erhalten
TA0007	Permissions Group Navigation	The actor uses the net localgroup administrator 〉〉 %temp%\download command after exploiting a computer with LOWBALL malware to list local groups

3.1.4. APT17 해커조직이 활용한 ATT&CK 기반의 공격 전술 및 소프트웨어

APT17 해커조직이 활용한 ATT&CK 기반의 공격 전술, 기법 및 소프트웨어 데이터를 구분 및 분석한 결과는 [표 10]과 같다[13].

〔표 10〕 ATT&CK 데이터 기반의 APT17 해커조직의 국가핵심기술 탈취 목적의 공격전술 및 공격기법 분석(일부)

Tactic	Technology	Explanation
TA0042	Hijacking infrastructure	Create a profile page on Microsoft TechNet used as C2 infrastructure

3.1.5. APT19 해커조직이 활용한 ATT&CK 기반의 공격 전술 및 소프트웨어

APT19 해커조직이 활용한 ATT&CK 기반의 공격 전술, 기법 및 소프트웨어 데이터를 구분 및 분석한 결과는 [표 11]과 같다[13].

〔표 11〕 ATT&CK 데이터 기반의 APT19 해커조직의 국가핵심기술 탈취 목적의 공격전술 및 공격기법 분석(일부)

Tactic	Technology	Explanation
TA0003 TA0004	Run boot or logon autostart	HTTP Malicious Code Variant Settings Persistence Registry Key Settings HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Debug Tools-%LOCALAPPDATA%\
TA0005	Artifact Hide Settings	Used to hide the PowerShell window -W Hidden by setting the WindowStyle parameter to hidden
TA0002	PowerShell	Run payload using PowerShell command
TA0005	Modify Registry	Modify multiple registry keys using port 22 Malicious Code variant
TA0003 TA0004 TA0005	Hijack Execution Flow : DLL side loading	Initiate HTTP Malicious Code Variants and Port 22 Malicious Code Variants using legitimate executable files loaded with Malicious DLLs
TA0001	Spear Phishing	Send spear phishing emails containing malicious attachments in RTF and XLSM formats to forward initial attacks
TA0007	System Information Navigating	System architecture information has been collected. APT19 collects hostname and CPU information from the victim's computer using HTTP malware variants and port 22 malware variants.

3.1.6. Bronze Butler 해커조직이 활용한 ATT&CK 기반의 공격 전술 및 소프트웨어

Bronze Butler 해커조직이 활용한 ATT&CK 기반의 공격 전술, 기법 및 소프트웨어 데이터를 구분 및 분석한 결과는 [표 12]과 같다[14][15].

〔표 12〕 ATT&CK 데이터 기반의 Bronze Butler 해커조직의 국가핵심기술 탈취 목적의 공격전술 및 공격기법 분석(일부)

Tactic	Technology	Explanation
TA0004 TA0005	Abuse Elevation Control Mechanism	권한 상승을 위해 UAC를 우회하기 위해 Windows 10 특정 도구와 xxmm를 사용
TA0007	Account Navigation	Search domain accounts including administrator accounts as net user /dom or net user administrator
TA0011	Application Layer Protocol: Web Protocol	Malicious code uses HTTP for C2
TA0009	Archive collected data: Archive through utility	Compress data into password-protected RAR archives prior to leakage
TA0002	Command and Scripting interpreters	Using Python-based remote access tools
TA0009	Data from the local system	Extracting files taken from the local system
TA0009	Data on a network shared drive	Extracting files taken from file shares
TA0001	Drive by Compromise	워터링홀 공격을 수행하기 위해 Flash 익스플로잇을 사용하여 3개의 일본 웹 사이트를 손상

3.2. ATT&CK 기반의 산업기술 유출방지 프레임워크 기술

현재 ATT&CK 기반의 사이버위협 대응 프레임워크는 주로 주요 해외 산업체에서 공동으로 발간하여 많이 활용하고 있다. 하지만, 국내에서의 활용빈도가 극히 낮으며 ATT&CK 데이터는 공격자에 대한 공격 전술, 기법, 대응 및 완화 정보 등 산업기술위협 대응과 유출 완화에 도움이 되는 중요 정보들이 데이터베이스화 되어 있다. 우리는 ATT&CK 데이터를 활용하여 산업기술위협을 대응할 수 있는 프레임워크를 체계화하여 국가핵심기술 유출을 최소화하고 완화할 수 있는 대응방안을 [그림 1]과 같이 제안하였다.

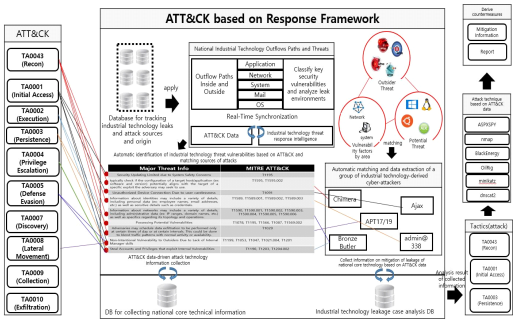
주요 연구 목표는 산업기술유출의 원인과 사례, 공격 출처, 침투 경로 등을 상관관계로 분석하여 실시간으로 동기화하여 공격전술에서 발생되는 유출사고 사례에 대해 ATT&CK 데이터 기반으로 공격 출처를 자동으로 매칭되고, 공격원점에 대한 역추적하여 완화하는 등 산업기술 유출을 감소시키는 것을 목표로 제안되었다.

산업기술유출 방지용 프레임워크는 다음과 같다. 산업기술 유출 사례와 공격 출처, 공격원점을 추적할 수 있는 데이터들을 수집하여 데이터베이스를 구축 및 활용한다.

수집된 데이터는 국가핵심기술 유출 경로 및 주요 위협 동향과 비교 분석하여 내/외부에서의 유출 경로, 주요 보안 취약점 분류 및 유출 환경 분석 데이터를 ATT&CK 전술단계와 산업기술 위협 대응 인텔리전스에 실시간적으로 동기화하여 산업기술 유출을 지속 관제를 수행한다.

관제를 통해 ATT&CK 전술과 연계된 산업기술 위협 취약점들을 식별 및 분류할 수 있고, 이를 통해 공격 출처 정보와 매칭되어 공격을 행한 공격자 정보, 공격자 의도 파악 등 데이터를 추출할 수 있다.

추출된 데이터를 활용하여 실시간적으로 동기화할 수 있도록 연동된 데이터베이스에 ATT&CK 데이터 기반의 공격 기술 정보와 국가핵심기술 유출 완화 정보를 수집 및 보관할 수 있다. 수집 및 보관된 정보들을 조사 및 분석을 수행하여 결과가 나오면 산업기술 유출 시도 시 활용된 공격전술과 공격기법, 절차, 결과를 로그형식으로 추출할 수 있다.



〔그림 1〕 ATT&CK Data 기반의 산업기술 유출방지용 프레임워크 체계화 설계

Ⅳ. 결 론

본 논문은 산업기술 유출 및 위협을 방지하고자 국가핵심기술 현황과 연도별 산업기술 유출 사례에 대해 분석하였다, 특히, MITRE社 ATT&CK 프레임워크, 산업기술탈취형 사이버공격자 그룹 프로파일링, 산업기술 유출 환경 분석 및 주요 방법, 주요 해커조직이 활용한 ATT&CK 기반의 공격전술, 기법, 절차 등 공격자 행위에 대해 분석하였고, 최근 사이버안보 뿐만 아니라 산업안보의 중요성이 대두되어 산업기술 유출 방지 및 위협 대응에 대해 연구하여 ATT&CK 프레임워크 기반의 산업기술위협 대응방안을 제안할 수 있었다. 본 논문을 통해 산업기술 유출사고에 대한 예방보안이 가능할 것으로 예상되며, 더 나아가 국가경쟁력 강화에 도움을 줄 것이라 기대된다.

참 고 문 헌

[1] 한국인터넷진흥원, “2021 국가정보보호백서”, *한국인터넷진흥원(KISA),* pp. 1-284, May 2021.

[2] 장항배, “산업기밀 유출사고 사례분석을 통한 유형별 대응방안 연구”, *융합보안논문지, 15*(7), pp. 39-45, December 2015.

[3] 국가정보원 홈페이지, https://www.nis.go.kr

[4] KISA, “CyberSecurity Issue Report: TTPs#1 Analysis of Internal Network Penetration Cases through the website”, Korea Internet & Security Agency (KISA), pp. 1-32, April. 2020.

[5] KISA, “CyberSecurity Issue Report: TTPs#2 How supply chain attacks are configured to gater in-

formation with spear phishing", Korea Internet & Security Agency (KISA), pp. 1-79, June. 2020.
[6] 안광현, 이한희, 박원형, 강지원, "국방 네트워크 환경에서 ATT&CK 기반 취약점 완화 체계 구축 방안", *융합보안논문지,* 20(4), pp. 135-141, October 2020.
[7] MITRE社 ATT&CK 홈페이지, https://attack.mitre.org/
[8] 국가법령정보센터, "산업기술의 유출방지 및 보호에 관한 법률 제9조(국가핵심기술의 지정, 변경 및 해제)", https://www.law.go.kr/
[9] 최응렬, "산업기술 유출경로 연구", *치안정책연구,* 26(1), pp. 225-259, March 2012.
[10] KISTI, "KISTI 침해사고 대응 분석 보고서", *한국과학기술정보연구원,* pp. 1-8, November 2015.
[11] FireEye, "M-TRENDS 2020", *FireEye Mandiant Trends Report,* pp. 1-60, 2020.
[12] FireEye, "China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Meida Outlets", *FireEye Threat Research,* January, 2015.
[13] FireEye, "APT37(REAPER) The Overlooked North Korean Actor", *파이어아이 위협 인텔리전스 보고서,* pp. 1-16, Feb 2018.
[14] ZDNet, "Mitsubishi Electric discloses security breach, China is main suspect"
[15] ESTsecurity, "유럽 은행 당국, 익스체인지 서버 해킹 알려", *이스트시큐리티 국내외 보안동향,* March 2021.

〈저 자 소 개〉

안 광 현 (Gwang-Hyun Ahn)
종신회원
2020년 9월~현재 : 세종대학교 컴퓨터공학 석·박사통합과정
2018년~2021년 : 국방부 국군 9965부대 침해사고대응팀 반장
2020년~2021년 : 한국산업보안연구학회 이사
2020년 5월~현재 : 한국정보보호학회 보안관제연구회 간사
2021년～현재 : 국가직 공무원 정보보호담당
<관심분야> 정보보호, 보안관제, 산업보안

오 재 헌 (JaeHeon Oh)
2021년 2월 : 건국대학교 정보보안학과 석사
2017년~2018년 : 윈스 보안관제팀 주임
2018년~2020년 : 행복마루컨설팅 디지털포렌식팀 매니저
2020년~현재 : 한국산업보안연구학회 이사
2020년~현재 : 딜로이트 안진회계법인, 리스크자문본부 컨설턴트
<관심분야> ISMS-P, digital Forensics, GITC, 산업보안

여 서 래 (Seorae Yeo)
2019년~현재 : 코리아서버호스팅 보안관제팀 매니저
<관심분야> 정보보안컨설팅, 산업보안, ISMS

박 원 형 (Won-Hyung Park)
종신회원
2002년 : 서울과학기술대학교 산업정보시스템 공학사
2005년 : 서울과학기술대학교 정보산업공학과 공학석사
2009년 : 경기대학교 정보보호학과 이학박사
2015년 : 성균관대학교 컴퓨터교육학과 박사수료
2012년~2020년 : 극동대학교 사이버보안학과 부교수/학과장
2020년~현재 : 상명대학교 정보보안공학과 부교수
<관심분야> 산업보안, 보안관제, Cyber Forensics