Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.4, Aug. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.4.673

MITRE ATT&CK을 이용한 APT 공격 스코어링 방법 연구

조 성 영,[1†‡] 박 용 우,[2] 이 건 호,[2] 최 창 희,[1] 신 찬 호,[2] 이 경 식[1]
[1,2]국방과학연구소 (선임연구원, 현역연구원)

An APT Attack Scoring Method Using MITRE ATT&CK

Sungyoung Cho,[1†‡] Yongwoo Park,[2] Kunho Lee,[2] Changhee Choi,[1]
Chanho Shin,[2] Kyeongsik Lee[1]
[1,2]Agency for Defense Development (Senior Researcher, Researcher)

요 약

본 연구에서는 APT 공격을 탐지하고 대응하기 위한 과정의 하나로 APT 공격을 스코어링하는 방안을 제안한다. 먼저, 사이버 공격을 스코어링하는 과정에서 비일관적인 전문가의 주관적인 판단 요소를 고려한 기존의 연구와는 달리, MITRE ATT&CK®의 공격기술을 구성하는 여러 구성요소 중 정량화할 수 있는 요소들을 식별하고 이를 정량화하는 방안을 제시한다. 또한, 정량화된 요소들을 이용하여 단위 공격기술의 스코어를 도출하고, 나아가 여러 공격기술로 구성된 전체 APT 공격의 스코어를 산출하는 방안을 제안한다. 제안한 스코어링 방법을 APT 공격 사례 보고서에 적용하여 APT 공격을 포함한 다양한 사이버 공격의 위협 수준 및 시급성을 판단하기 위한 정량화 가능성을 제시한다. 본 연구를 이용하여 APT 공격을 탐지하는 과정에서 실제 공격 여부를 판단하고, 공격의 우선순위를 산정함으로써 더욱 시급하고 중요한 사이버 공격에 대응할 수 있을 것이다.

ABSTRACT

We propose an APT attack scoring method as a part of the process for detecting and responding to APT attacks. First, unlike previous work that considered inconsistent and subjective factors determined by cyber security experts in the process of scoring cyber attacks, we identify quantifiable factors from components of MITRE ATT&CK® techniques and propose a method of quantifying each identified factor. Then, we propose a method of calculating the score of the unit attack technique from the quantified factors, and the score of the entire APT attack composed of one or more multiple attack techniques. We present the possibility of quantification to determine the threat level and urgency of cyber attacks by applying the proposed scoring method to the APT attack reports, which contains the hundreds of APT attack cases occurred worldwide. Using our work, it will be possible to determine whether actual cyber attacks have occurred in the process of detecting APT attacks, and respond to more urgent and important cyber attacks by estimating the priority of APT attacks.

Keywords: MITRE ATT&CK, Techniques, Scoring, Quantification, Threat Prioritization

I. 서 론

표적 공격(targeted attack) 또는 APT(advanced persistent threat) 공격과 같은 사이버 공격은 국가 또는 조직의 후원 아래 기밀 탈취, 데이터 및 시스템의 무결성 또는 가용성 파괴 등과 같은 궁극적

Received(05. 25. 2022), Modified(07. 01. 2022), Accepted(07. 06. 2022)

† 주저자, sycho@add.re.kr
‡ 교신저자, sycho@add.re.kr(Corresponding author)

인 공격 목표를 달성하기 위해 수행된다. 이 과정에서 공격자들은 다양한 공격 방법들을 이용하여 여러 공격 단계들로 구성된 작전(operations) 형태로 수개월 또는 수년의 시간 동안 사이버 공격을 수행하는 것으로 추측되고 있다.

사이버 공격을 효과적으로 탐지하고 대응하기 위한 노력의 하나로, MITRE 社에서 발표한 ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) 프레임워크[6, 7]는 사이버 공격의 전술, 기술 및 절차(TTPs, tactics, techniques, and procedure)를 설명할 수 있는 사실상 표준 모델로 자리 잡고 있다. ATT&CK 프레임워크를 이용하여 APT 공격을 효과적으로 탐지하고 대응하기 위한 여러 연구[1, 2, 4]가 있으며, 특히 이들은 APT 공격을 스코어링(scoring)하는 방법을 제안하였다. 그러나 연구마다 공격의 수준을 스코어링하는 목적과 방법이 모두 다르며, 스코어링 과정에서 주관적인 요소에 의존하기도 한다.

본 연구에서는 APT 공격을 스코어링하는 방법을 제안한다. 다른 연구들과는 달리 주관적인 요소를 포함하지 않고 ATT&CK 프레임워크가 포함하는 정보를 전적으로 활용하는 스코어링 방법을 제안한다. 먼저 ATT&CK의 각 공격기술을 스코어링하고, 이를 이용하여 여러 공격기술로 구성된 전체 APT 공격을 스코어링한다.

2장에서는 관련 연구를 살펴보면서 공격 스코어링 접근방법 및 그 한계를 지적한다. 3장에서는 MITRE ATT&CK 프레임워크를 살펴보고, 공격기술의 구성요소 중 정량화할 수 있는 요소를 식별하고 이를 이용하여 공격을 스코어링하는 방법을 제안한다. 4장에서는 3장에서 제안한 스코어링 방법을 이용하여 주요 APT 공격을 분석한 위협 인텔리전스(threat intelligence) 보고서를 이용하여 APT 공격을 스코어링한 결과를 제시한다. 5장에서는 결론과 개선 방안을 포함한 향후 연구 방향을 제시한다.

II. 관련 연구

HOLMES[1]에서는 APT 공격을 탐지하기 위하여 공격기술을 스코어링한다. 이를 위해 APT 공격을 설명하는 대표적 모델인 록히드 마틴 社의 사이버 킬체인[3]의 7단계, 즉 정찰(reconnaissance), 무기화(weaponization), 유포 및 침투(delivery), 익스플로잇(exploitation), 설치(installation), 명령 및 제어(command and control), 목적 달성(actions on objectives)의 단계별 공격기술의 심각도 수준 중 가장 큰 값을 부여한다. 각 공격기술은 MITRE ATT&CK[7]에 정의된 공격기술을 이용하며, 각 공격기술의 심각도는 연관된 CAPEC (Common Attack Pattern Enumeration and Classification)[8]의 공격패턴에 정의된 일반적 심각도(typical severity)를 이용한다. 단, 상황에 따라 분석가의 목적에 맞게 수정(tailor)한 심각도 수준을 사용할 수도 있으며, 각 단계에 대한 상대적 중요도를 반영하여 분석가에게 맞춘 가중치를 산정할 수 있다. 각 공격기술의 심각도 수준은 Table 1.과 같이 정성적 수준(qualitative level)에서 정량적 범위(quantitative range)로 환산하고, 그 값을 이용하여 다음의 식 (1)에 따라 APT 공격의 스코어를 계산하여, 그 값이 임계치(τ) 이상일 때 APT 공격을 탐지한다. 여기서 n은 APT 공격을 구성하는 전체 단계(7단계), w_i와 S_i는 각 공격 단계에서의 가중치 및 최대 심각도를 나타낸다.

Table 1. Conversion table from qualitative level to quantitative value[1]

Qualitative level	Quantitative range	Rounded up Average value
Low	0.1-3.9	2.0
Medium	4.0-6.9	6.0
High	7.0-8.9	8.0
Critical	9.0-10.0	10.0

$$\prod_{i=1}^{n}(S_i)^{w_i} \geq \tau \quad (1)$$

Hassan 등의 연구[2]에서는 상용 EDR (endpoint detection and response) 제품에서 발생하는 경보(alert)를 이용하여 Provenance Graph를 도출하고 이를 Tactical Provenance Graph(TPG)로 명명한다. 그 과정에서 각 경보는 MITRE ATT&CK의 공격기술에 매핑되며, 해당 ATT&CK의 공격기술과 연관된 CAPEC 공격패턴의 일반적 심각도 및 공격 가능성(likelihood of attack) 정보를 이용하여 해당 경보를 스코어링한다. 일반적 심각도와 공격 가능성은 5가지의 값(very low, low, medium, high, very high)을 가질 수 있으며, 이를 각각 [1, 5]점 범위의 점수로 환산한다. ATT&CK 공격기술 중 연관된 CAPEC

Table 2. Comparison of related work

Ref.	Objective	Main quantification factors	Weight	Use subjective factors	Calculation method
[1]	Calculate the score of high-level scenario graph (HSG) that cyber kill chain concept is applied, and detect an APT attack if the score is greater than the predefined threshold.	☑ Associated CAPEC attack pattern ▪ Typical severity	Lockheed Martin Cyber Kill Chain phases[3]	O	Multiplication of the maximum score of each attack phase weighted by corresponding phase.
[2]	Calculate the threat score for the tactical provenance graph which consists of alerts generated from EDR tools to triage contextualized alerts (tactical provenance graph).	☑ Associated CAPEC attack pattern ▪ Typical severity ▪ Likelihood of attack	X	O	Weighted sum for individual alert, and multiplication of all alerts in all subgraphs in the tactical provenance graph, and take the maximum value.
[4]	To prioritize the observed cyber threat (rule-based attack mapped to MITRE ATT&CK) detected by threat hunting.	☑ User-defined risk level ☑ Associated CAPEC attack pattern ▪ Typical severity ▪ Likelihood of attack	X	O	Weighted sum of quantification factors (not defined for an entire APT attack, but for individual attack).
Ours	To prioritize the ATT&CK techniques, and calculate the score of attack chain reconstructed[15] to detect an APT attack.	☑ Attributes of MITRE ATT&CK Techniques ☑ Associated CAPEC attack pattern ▪ Typical severity	MITRE ATT&CK Tactics	X	Average the non-zero attributes for each technique and weight by corresponding tactic, then sum all techniques contained in an entire APT attack.

공격패턴이 존재하지 않거나, CAPEC 공격패턴 중 일반적 심각도 또는 공격 가능성의 값이 없는 경우 EDR 제조사가 부여한 심각도 점수를 이용하여 15단계 범위에서 정규화한다.

CAPEC 공격패턴을 이용한 각 공격기술의 심각도는 다음의 식 (2)에 따라 계산한다.

$$TS(\text{technique}) = 2 \times score_{\text{severity}} + score_{\text{likelihood}} \quad (2)$$

EDR에서 탐지하여 발생한 경보를 이용하여 TPG를 생성하면, TPG를 구성하는 여러 경로 중 가장 긴 경로(Y)에 대해 다음의 식 (3)에 따라 TPG, 즉 전체 위협의 스코어를 계산한다. 최종 스코어는 TPG 중 가장 긴 경로상에 있는 모든 경보에 해당하는 공격기술의 심각도를 모두 곱한 값이다.

$$TS(\text{TPG}) = \max_{\mathbf{T^i} \in Y} \prod_{T_j^i \in \mathbf{T^i}} TS(T_j^i) \quad (3)$$

다른 연구[4]에서는 공격의 우선순위를 산정하기 위해서 공격을 탐지 또는 식별하기 위한 규칙[9]에 사용자 정의된 위험 수준(risk level), 연관된 ATT&CK 공격기술이 있는 경우 해당 공격기술과 연관된 CAPEC의 공격패턴에 정의된 일반적 심각도와 공격 가능성을 이용하여 규칙의 위험도를 다음의 식 (4)에 따라 계산한다. 여기서 α와 β는 $[0, 1]$ 사이의 값으로 조정할 수 있다.

$$t_{RISK} = \beta \times (\alpha \times score_{\text{likelihood}} + (1-\alpha) \times score_{\text{severity}}) + (1-\beta) \times score_{\text{custom}} \quad (4)$$

기존 연구들이 제안한 스코어링 방법은 Table 2.와 같이 요약할 수 있다. 한편 이들의 문제점은 다음과 같다. 첫째, 공통으로 참조하는 CAPEC의 모든 공격패턴이 일반적 심각도와 공격 가능성에 대한 값을 가지고 있지는 않다. 전체 601개의 CAPEC의 공격패턴 중 일반적 심각도와 공격 가능성에 대한 값을 가진 공격패턴은 각각 475개와 330개에 불과하다.

둘째, Hassan 등[2]도 언급하고 있듯이, ATT&CK과 연관된 CAPEC이 있는 경우는 527개의 공격기술 중 108개에 불과하다. 게다가, CAPEC 중 일반적 심각도 또는 공격 가능성을 모두 가지고 있지는 않기 때문에 기존 연구[1, 2, 4]에서 일반적 심각도 또는 공격 가능성에 비어 있는 값(null 값)에 대해서 사용자(분석가)가 수치를 부여한다.

셋째, 분석가가 수치를 부여할 때 분석가의 개인적인 편향에 따라 주관적으로 스코어가 산정되므로[5], 서로 다른 분석가에 의해 부여된 스코어는 상호 비교할 수 없다는 문제가 있다.

Table 3. Tactics in MITRE ATT&CK[6], and number of (sub-)techniques in each tactic

ID	Name	Description	Technique	Sub-Technique	Total
TA0043	Reconnaissance	To gather information to plan future operations	10	31	41
TA0042	Resource Development	To establish resources to support operations	7	31	38
TA0001	Initial Access	To get into victim network	9	10	19
TA0002	Execution	To run malicious code	12	21	33
TA0003	Persistence	To maintain adversaries' foothold	19	87	106
TA0004	Privilege Escalation	To gather higher-level permissions	13	82	95
TA0005	Defense Evasion	To avoid being detected	40	124	164
TA0006	Credential Access	To steal account names and passwords	15	40	55
TA0007	Discovery	To figure out victim's environment	29	13	42
TA0008	Lateral Movement	To move through victim's environment	9	12	21
TA0009	Collection	To gather data of interest to adversaries' goal	17	19	36
TA0011	Command and Control	To communicate with compromised systems to control them	16	22	38
TA0010	Exfiltration	To steal data	9	8	17
TA0040	Impact	To manipulate, interrupt, or destroy victim's system or data	13	13	26

III. 공격 스코어링

3.1 MITRE ATT&CK

MITRE ATT&CK[6, 7]은 전세계에서 발생한 사이버 공격의 사례를 분석하여 정리한 위협 인텔리전스(threat intelligence)로, 공격자가 수행하였거나 수행할 수 있는 공격 TTPs 및 이들을 사용한 공격 그룹(group)들과 소프트웨어(악성코드 및 정상 도구들), 각 공격기술을 탐지(detection)하고 완화(mitigation)하는 방법, 각 공격기술을 탐지하기 위해 사용할 수 있는 데이터 소스(data source)와 데이터 컴포넌트(data component)로 구성되어 있다.

ATT&CK의 TTPs는 공격자가 달성하고자 하는 단기적인 목적에 해당하는 전술(tactics), 해당 전술을 위해 사용할 수 있는 (세부) 공격기술((sub-)technique, 각 전술에 속한 공격기술들의 분포는 Table 3.과 같다), 식별된 공격 그룹 또는 소프트웨어가 구체적으로 각 공격기술을 사용한 방법(또는 절차, procedures)들로 구성되어 있다.

3.2 공격기술 스코어링 요소

ATT&CK의 공격기술에는 각각을 설명하고 분류할 수 있도록 Table 4.[6]와 같은 구성요소들을 포함하며, 이 중 주관적인 판단이 개입될 여지가 있는 요소(예. 탐지 방법, 완화 방법)와 객관적으로 비교할 수 없는 유형값을 갖는 요소(예. 영향 유형(impact type))를 제외하고 객관적인 스코어링이 가능한 요소들을 Table 5.와 같이 식별하였다.

Table 4. Properties of ATT&CK techniques[6]

Field	Description
Name	The name of (sub-)technique
ID	Unique Identifier for the (sub-)technique
Tactic	The tactic objectives that the (sub-)technique can be used to accomplish
Description	Information about the (sub-)technique
Platform	The system an adversary is operating within
System Requirements	Additional information on requirements the adversary needs to meet or about the state of the system that may be required for the (sub-)technique to work
Network Requirements	Whether the network connection is required for the (sub-)technique to work
Permission Required	The lowest level of permissions the adversary is required to be operating within to perform the (sub-)technique on a system
Effective Permissions	The level of permissions the adversary will attain by performing the (sub-)technique
Data Sources	Source of information collected by a sensor or logging system that may used to collect information relevant to identifying the acting being performed, sequence of actions, or the results of those actions by an adversary
Supports Remote	Whether the (sub-)technique can be used to execute something on a remote system
Defense Bypassed	Whether the (sub-)technique can be used to bypass or evade a particular defensive tool
CAPEC ID	Related CAPEC[3] entries
Impact Type	If the (sub-)technique can be used for integrity or availability attacks
Procedure Example	The group or software entity with a brief description of how the (sub-)technique is used
Detection	High level analytic process, sensors, data, and detection strategies that can be useful to identify a (sub-)technique has been used by an adversary
Mitigation	Configurations, tools, or process that can prevent a (sub-)technique from working or having the desired outcome for an adversary

Table 5. Quantifiable factors applicable to each tactic

Tactics	Tactic	Platform	Permission Required	Effective Permission	Data Sources	Supports Remote	Defense Bypassed	CAPEC Severity	Procedure Examples	Total Number of factors considered
Reconnaissance	X	X	X	X	O	X	X	If exists	O	3
Resource Development	X	X	X	X	O	X	X	If exists	O	3
Initial Access	O	O	O	X	O	X	X	If exists	O	6
Execution	O	O	O	X	O	O	X	If exists	O	7
Persistence	O	O	O	X	O	X	X	If exists	O	6
Privilege Escalation	O	O	O	O	O	X	X	If exists	O	7
Defense Evasion	O	O	O	X	O	X	O	If exists	O	7
Credential Access	O	O	O	X	O	X	X	If exists	O	6
Discovery	O	O	O	X	O	X	X	If exists	O	6
Lateral Movement	O	O	O	X	O	X	O	If exists	O	7
Collection	O	O	O	X	O	X	X	If exists	O	6
Command and Control	O	O	O	X	O	X	X	If exists	O	6
Exfiltration	X	O	O	X	O	X	X	If exists	O	5
Impact	X	O	O	X	O	X	X	If exists	O	5

또한, 전술별로 특정 구성요소가 각 공격기술을 스코어링 하는 데 영향을 미치지 않는 요소는 전술별로 제외하였다. 예를 들어, 정찰(reconnaissance)과 자원 개발(resource development)에 속한 공격기술의 플랫폼(platforms) 개수가 모두 같으며, 플랫폼의 값이 모두 'PRE'로서, 초기 접근(initial access) 전술 이후의 공격기술의 플랫폼 값이 Windows, Linux, macOS 등과 같은 실질적인 공격대상 플랫폼인 점과 비교하면 실질적으로 플랫폼의 값이 없는 것과 마찬가지이므로, 정찰과 자원 개발 전술에서 플랫폼 요소를 스코어링 요소에서 배제하였다.

3.2.1 전술 (tactic)

정찰, 자원 개발, 유출(exfiltration), 영향(impact) 전술을 제외한 나머지 전술에 속한 공격기술 중 두 가지 전술 이상에 속한 것들은 한 가지의 전술에 속한 것보다 더 많은 목적에 사용될 수 있어 활용도가 높으므로 (공격 활용성) 더 큰 점수를 부여할 수 있다. 이때 점수는 다음의 식 (5)를 이용하여 계산할 수 있으며, [1, 5]점 범위 내에서 부여된다.

$$score_{\text{tactic}} = 1 + (\text{num}_{\text{tactic}} - 1) \quad (5)$$

여기서 $\text{num}_{\text{tactic}}$은 해당 공격기술이 속한 전술의 개수이다. 정찰, 자원 개발, 유출, 영향 전술의 공격기술에 대해서는 0점이 부여된다.

3.2.2 플랫폼 (platform)

정찰, 자원 개발 전술을 제외한 나머지 전술에 속한 공격기술 중 여러 공격대상 플랫폼에 대한 것들은 한 가지의 공격대상 플랫폼에 대한 것보다 활용도가 높으므로 (공격 표면) 더 큰 점수를 부여할 수 있다. 수치는 한 가지의 공격대상 플랫폼일 경우 1점, 두 가지 이상의 공격대상 플랫폼일 경우 5점이 부여된다. 정찰, 자원 개발 전술의 공격기술에 대해서는 0점이 부여된다.

3.2.3 요구 권한 (required permissions)

정찰, 자원 개발 전술을 제외한 나머지 전술에 속한 공격기술 중 요구 권한 항목에 대한 값이 존재하는 경우, 목록에 나열된 것 중 가장 낮은 값이 부여된다. 요구 권한에는 Table 6.의 항목 중에 해당하며, (1) root와 Administrator는 각각 Linux, macOS, Windows 운영체제에서의 관리자 수준의 계정이나, (2) Windows에서는 SYSTEM이 시스템에서 최고 권한을 가진 계정이며, 로컬에서 관리자

Table 6. Quantification of required permissions and permission effective

Value	Quantification Value
SYSTEM	5
root (for Linux, macOS)	5
Administrator (for Windows)	3
User	1
Remote Desktop User	1

보다 상위 수준의 권한을 갖는다는 점, (3) Linux 및 macOS에서는 root가 SYSTEM 대신 시스템에서 최고 권한을 가지는 점 등을 반영하여 각 항목은 [1, 5]점 범위 내에서 부여된다. Remote Desktop User는 내부 확산(lateral movement) 전술의 T1021.001(Remote Services: Remote Desktop Protocol)에만 나타나는 값으로, 권한 여부와 무관하게 원격 시스템에 접속하는 행위이므로 일반 사용자와 같이 간주한다. 한편, 정찰, 자원 개발 전술의 공격기술에 대해서는 0점이 부여된다.

3.2.4 획득 권한 (effective permissions)

권한 상승(privilege escalation) 전술에 속한 공격기술만이 가지고 있는 요소로, 특정 공격기술을 수행함으로써 공격자가 얻을 수 있는 권한 수준을 의미한다. 획득 권한 수준이 높을수록 공격의 위험도가 높음을 의미한다. 획득 권한에는 Table 6.의 항목 중에 해당하며, 각 항목은 [1, 5]점 범위 내에서 부여되며, 목록에 나열된 것 중 가장 큰 값이 부여된다. 권한 상승 전술을 제외한 나머지 전술의 공격기술에 대해서는 0점이 부여된다.

3.2.5 데이터 소스 (data sources)

데이터 소스는 공격기술을 탐지하는 데 필요한 데이터의 종류(category) 및 유형(type)을 의미한다. 특정 공격기술에 대한 데이터 소스의 항목이 많을수록 이를 탐지할 가능성이 크며, 해당 공격기술에 대한 공격의 영향을 감소시킬 수 있다. 따라서 데이터 소스가 많을수록 데이터 소스 항목에 대한 수치를 감소시킴으로써 공격 수준에 대한 전반적인 수치를 감소시킬 수 있다고 판단하였다. 따라서 수치는 다음과 같이 부여된다.

- 데이터 소스가 한 종류이며, 그 안의 데이터 컴포넌트가 한 개: 5점
- 데이터 소스가 한 종류이며, 그 안의 데이터 컴포넌트가 두 개 이상: 3점
- 데이터 소스가 두 종류 이상: 1점

3.2.6 원격 지원 (remote supports)

실행(execution) 전술에 속한 공격기술만 가지고 있는 요소로, 특정 공격기술을 원격 시스템에서 실행할 수 있는지를 나타낸다. 만약 해당 공격기술이 원격으로 실행될 수 있다면 그 공격기술은 다른 공격기술보다 위험도가 높음을 의미한다. 따라서 예(yes)에 해당하면 5점, 아니오(no)에 해당하면 1점이 부여된다. 실행 전술을 제외한 나머지 전술의 공격기술에 대해서는 0점이 부여된다.

3.2.7 방어 우회 (defense bypassed)

방어 회피(defense evasion) 및 내부 확산(lateral movement) 전술에 속한 공격기술만 가지고 있는 요소로, 공격자가 해당 공격기술을 사용함으로써 우회하고자 하는 여러 방어 기술을 열거한다. 여러 우회 방법들이 나열된 공격기술은 그만큼 은밀하게 수행될 가능성이 크므로 다른 공격기술보다 위험도가 높음을 의미한다. 먼저 방어 우회 항목에 나열된 대상 방어 기술을 Table 7.과 같이 호스트 기

Table 7. Defensive mechanisms enumerated in 'Defense Bypassed' field

Category	Defensive Mechanism
Host	• Anti-Virus • Application Control • Application Control by File Name or Path • Autoruns Analysis • Binary Analysis • Digital Certificate Validation • File Monitoring • File System Access Controls • Heuristic Detection • Host Forensic Analysis • Host Intrusion Prevention Systems • Log Analysis • Notarization: Gatekeeper • Static File Analysis • System Access Controls • User Mode Signature Validation • Windows User Account Control
Network	• Encryption • Firewall • Router ACL • Network Intrusion Detection System • Signature-based Detection • Web Content Filters

반 방어 기술과 네트워크 방어 기술로 구분하고 수치는 다음과 같이 부여된다.

- 방어 우회 기법의 대상 종류가 한 종류: 1점
- 방어 우회 기법의 대상 종류가 한 종류이며, 그 안의 방어 기법이 두 개 이상: 3점
- 방어 우회 기법의 대상 종류가 두 종류 이상: 5점

방어 회피 및 내부 확산 전술을 제외한 나머지 전술에 속한 공격기술에 대해서는 0점이 부여된다.

3.2.8 CAPEC ID

CAPEC[8]은 공격자가 애플리케이션 및 기타 사이버 기반 기능의 취약점을 악용하는 방법(공격패턴)에 대한 프레임워크로, 미국 국토안보부(DHS, Department of Homeland and Security)의 소프트웨어 보증(software assurance) 전략의 일부로써 MITRE 社에서 2007년 최초로 발표하였다. ATT&CK은 APT 공격에 대한 공격기술을 다루지만, CAPEC은 애플리케이션에 대한 공격패턴을 다룬다는 점에서 차이가 있다. 그러나 ATT&CK의 공격기술과 CAPEC의 공격패턴 중 세부적으로 유사한 것들이 존재한다.

CAPEC 공격패턴의 구성요소는 Table 8.과 같다. 이 중 수치화할 수 있는 구성요소는 사전 조건(prerequisites), 결과(consequences), 공격 가능성, 요구 기술(skills required), 일반적 심각도가 있으며, 이 중 사전 조건을 제외한 나머지 구성요소는 5단계(very low, low, medium, high, very high)의 값으로 구성되어 있어 수치화하기 쉽다. 그러나 Table 9.에서 볼 수 있듯이, 일반적 심

Table 8. Properties of CAPEC attack patterns[8]

Field	Description	Remark
Name	Name of an attack pattern	
Description	Description of an attack pattern	
Example Instances	Example instances of an attack pattern	
Execution Flows	Step-by-step execution flows of an attack pattern	
Prerequisites	One or more prerequisites of an attack pattern	
Consequences	Consequences of an attack pattern	High, Medium, Low
Likelihood of Attack	Likelihood of occurrence of an attack pattern	High, Medium, Low
Skills Required	Levels and their detailed skills required to perform an attack pattern	High, Medium, Low
Typical Severity	Typical severity of an attack pattern	High, Medium, Low
Related Weakness	Related CWE IDs of an attack pattern	
Mitigation	Actions or approaches to prevent or mitigate an attack pattern	

Table 9. Number of (sub-)techniques mapped to CAPEC attack patterns, and number of (sub-)techniques containing CAPEC quantifiable factors by ATT&CK tactic

Tactic ID	Tactic Name	Number of techniques			Number of techniques containing CAPEC factors				
		Total	CAPEC mapped	%	Typical Severity	Likelihood of attack	Skills Required	Prereq-uisites	Conseq-uences
TA0042	Reconnaissance	41	1	2.44%	1	1	1	1	1
TA0043	Resource Development	38	1	2.63%	1	1	1	1	1
TA0001	Initial Access	19	11	57.89%	10	9	8	9	9
TA0002	Execution	33	2	6.06%	1	1	0	0	1
TA0003	Persistence	106	34	32.08%	26	21	17	22	18
TA0004	Privilege Escalation	95	35	36.84%	26	22	19	24	20
TA0005	Defense Evasion	164	45	27.44%	44	33	29	40	29
TA0006	Credential Access	55	17	30.91%	14	10	12	14	13
TA0007	Discovery	42	19	45.24%	18	13	7	17	17
TA0008	Lateral Movement	21	13	61.90%	11	7	7	7	8
TA0009	Collection	36	13	36.11%	11	7	7	10	8
TA0010	Exfiltration	17	1	5.88%	1	1	0	1	1
TA0011	Command and Control	38	3	7.89%	3	1	1	2	1
TA0040	Impact	26	8	30.77%	7	6	4	8	6

각도 외의 다른 요소들에 대해 null 값을 가진 CAPEC 공격패턴이 많으며, 사전 조건, 결과, 요구 기술은 그 값들의 우열을 가릴 수 없는 유형값들로 구성되어 있어 수치화가 어렵다. 예를 들어, 결과 항목에서는 기밀성(confidentiality), 무결성(integrity), 가용성(availability), 접근제어(access control) 등의 유형과 그 유형에 대한 세부 결과를 제시하는데, 기밀성, 무결성, 가용성 간의 우열을 비교하는 것은 매우 어렵다. 따라서 대부분의 CAPEC 공격패턴이 포함하고 있으면서 공격패턴의 수준을 확인할 수 있는 일반적 심각도만을 이용한다.

일반적 심각도에 대한 수치는 Table 10.을 이용하여 부여한다. 특정 공격기술에 매칭되는 CAPEC 공격패턴이 두 개 이상이면 가장 높은 일반적 심각도를 대푯값으로 부여하며, 매칭되는 CAPEC 공격패턴이 있으나 이의 일반적 심각도 값이 부여되지 않은 경우, 또는 매칭되는 CAPEC 공격패턴이 없는 공격기술에 대해서는 0점이 부여된다.

그러나 CAPEC 공격패턴과 연관된 ATT&CK 공격기술은 전체 566개 중 134개(23.67%)로, 전술별로는 Table 9.와 같은 분포를 보인다. 정찰, 자원개발, 실행, 유출, 명령 제어 전술에 속한 공격기술 중 CAPEC 공격패턴과 연관된 공격기술의 비율이 10% 미만으로 나타난다. 따라서 매칭되는 CAPEC 공격패턴이 없으나 일반적으로 높은 수준의 심각도라고 판단되는 공격기술에 대해서 0점이 부여됨으로써, CAPEC 공격패턴이 존재하고 이의 일반적 심각도 값이 낮은(low) 공격기술보다 심각도가 낮게 평가되는 문제가 발생한다.

이러한 문제를 해결하기 위해, CAPEC 공격패턴 속성에 대해 0점이 부여되었을 때 CAPEC 공격패턴 속성을 해당 공격기술의 스코어링 요소에서 배제한다. 이는 CAPEC 공격패턴이 있고 일반적 심각도 값이 부여된 공격기술과의 형평성을 위한 조치이다.

Table 10. Quantification of CAPEC typical severity

Value	Quantification Value
Very High	5
High	4
Medium	3
Low	2
Very Low	1
None	0

3.2.9 절차 사례 (procedure example)

절차 사례는 모든 공격기술이 공격 그룹, 악성코드 및 정상적인 목적의 도구를 포함한 소프트웨어에 의해 사용된 사례들을 모아 놓은 것이며, ATT&CK에서는 위협 분석 보고서, 블로그 게시글 등 공개된 위협 인텔리전스를 분석하여 공격기술마다 정리하였다. ATT&CK에서 가장 많은 절차 사례들을 포함하고 있는 10개의 공격기술은 Table 11.과 같다.

ATT&CK 공격기술에 나열된 절차 사례를 분석하여 Table 12.와 같이 절차 사례 수에 따른 공격기술 수의 분포를 도출하였다. 구체적으로는, 절차 사례 수가 10개 이하인 공격기술은 400개로 전체의 70.67%를 차지하며, 이 중 343개가 각각 0개(123개 공격기술), 1개(77개 공격기술), 2개(71개 공격기술), 3개(30개 공격기술), 4개(26개 공격기술), 5개(16개 공격기술)의 절차 사례를 포함하고 있다. 또한 대다수(522개, 전체의 92.33%) 공격기술은 최대 50개의 절차 사례를 포함하고 있어, 매우 소수의 공격기술이 절대적으로 많이 사용되고 있음을 볼 수 있다.

또한 ATT&CK 공격기술에 나열된 절차 사례 수에 대한 통계량은 Table 13.과 같다. 이를 이용하여 전체 ATT&CK 공격기술의 절차 사례 수에 대한 스코어는 [0,5]점의 범위에서 다음의 식 (6)에

Table 11. Top 10 most populated procedure examples of (sub-)techniques

Technique ID	Technique Name	Number of Procedures
T1105	Ingress Tool Transfer	337
T1082	System Information Discovery	283
T1027	Obfuscated Files or Information	275
T1059.003	Command and Scripting Interpreter: Windows Command Shell	260
T1071.001	Application Layer Protocol: Web Protocols	259
T1083	File and Directory Discovery	240
T1057	Process Discovery	206
T1070.004	Indicator Removal on Host: File Deletion	200
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	196
T1016	System Network Configuration Discovery	193

Table 12. Histogram of the number of (sub-)techniques according to the number of procedure examples

Number of procedure examples	Number of (sub-)techniques
0~10	400
11~20	54
21~30	33
31~40	20
41~50	15
51~60	7
61~70	6
71~80	3
81~90	3
91~100	3
101~150	11
151~200	4
200~250	2
250~300	4
300~350	1

따라 부여된다.

$$score_{procedures} = \frac{num - bound_{upper}}{bound_{upper} - bound_{lower}} \times 5 \quad (6)$$

여기서 'num'은 해당 공격기술의 절차 사례 수, $bound_{upper}$과 $bound_{lower}$은 각각 Table 13.의 Upper bound와 Lower bound이다. Upper bound를 넘는 절차 사례 수는 이상값(outlier)으로 간주하고 최대 점수인 5점을 부여한다.

Table 13. Statistics of the number of procedure examples

Minimum	0
Median	3
Maximum	337
Average	16.5795053
Standard Deviation	38.8540333
Ql (Bottom 25%)	1
Q3 (Top 25%)	14
IQR (Interquartile range)	3
Lower bound (Q1-1.5×IQR)	0
Upper bound (Q3+1.5×IQR)	33.5

3.2.10 요약

ATT&CK 공격기술의 구성요소 중 정량화할 수 있는 9가지의 요소들, 즉 전술, 플랫폼, 요구 권한, 획득 권한, 데이터 소스, 원격 지원, 방어 우회, 연관된 CAPEC 공격패턴의 일반적 심각도, 절차 사례 수를 식별하였다. 각 요소 및 스코어링 방법은 Table 14.와 같이 요약하였다.

Table 14. Quantifiable factors to score individual ATT&CK (sub-)technique

Factor	Scoring Method	Exclusive Tactics
Tactic	1 + (number of tactics - 1)	
Platform	more than one: 5, one: 1	
Required Permission	root/SYSTEM: 5, Administrator: 3, User: 1 The lowest value in the 'Required Permission' list in individual (sub-)technique	
Effective Permission	root/SYSTEM: 5, Administrator: 3, User: 1 The highest value in the 'Effective Permission' list in individual (sub-)technique	Privilege Escalation
Data Sources	One data source, one data component: 1 One data source, more than one component: 3 More than one data source: 5	
Supports Remote	Yes: 5, No: 1	Execution
Defense Bypassed	Categorize by Table 7 One category, one method: 5 One category, more than one method: 3 More than one category: 1	Defense Evasion Lateral Movement
CAPEC Severity	Related CAPEC's typical severity, if more than one, the highest one. Very High: 5, High: 4, Medium: 3, Low: 2, Very Low: 1	If no value found, do not account for scoring
Procedure Examples	For whole (sub-)technique, derive Q1, Q3, IQR, and lower/upper bound for box plot. Then calculate for individual (sub-)technique (number of procedure examples - lower bound)/(upper bound-lower bound) * 5 If the the number of procedure examples is grater than upper bound, set to 5.	

3.3 단위 공격기술 스코어링

3.3.1 전술 가중치

3.2장에서 언급한 스코어링 요소는 공격기술이 속한 전술의 속성을 고려하지 않았다. 그러나 실제로 전술은 공격자의 공격 목표와 연계되어 다르게 평가되어야 한다. 예를 들어, 초기 접근 전술은 공격 초기에 수행되는 단계이며, 유출 및 영향 단계는 공격의 최종목표에 해당하는 단계이므로 두 단계에 대한 우선순위와 가중치는 다르게 부여되어야 한다. 따라서 각 전술은 목적의 시급성과 영향도에 따라서 다른 우선순위와 그에 따른 가중치가 부여된다.

전술 간의 우선순위는 미국 국가안보국(NSA, National Security Agency)에서 발표한 바 있는 Technical Cyber Threat Framework[10]의 주요 단계를 참고하여 산정하였다. ATT&CK 프레임워크를 기반으로 만들어진 Technical Cyber Threat Framework의 주요 공격 단계는 관리(administration, 자원 개발 전술에 해당), 준비(preparation, 정찰 및 자원 개발 전술에 해당), 교전(engagement, 초기 접근 전술에 해당), 출현(presence, 실행, 발견, 권한 상승, 자격증명 접근, 내부 확산, 지속 유지 전술에 해당), 효과(effect, 수집, 유출, 영향 전술에 해당), 진행 중 프로세스(ongoing processes, 명령 및 제어, 방어 회피 전술에 해당)로 구성되어 있다.

가장 높은 우선순위(1)를 갖는 전술은 APT 공격의 궁극적인 목표에 해당하는 유출(기밀성 훼손) 및 영향(무결성 또는 가용성 훼손)이다.

두 번째로 높은 우선순위(2)를 갖는 전술은 APT 공격의 궁극적인 목표는 아니지만, 공격자가 수행할 때 매우 큰 심각한 위협이 되는 전술로, 내부 확산(APT 공격의 궁극적 목표가 되는 자산으로 공격 목표를 이동한다), 자격증명 접근(시스템 또는 관리자 계정 획득 시 APT 공격의 궁극적 목표를 달성할 수 있다), 수집(유출 전술에 대한 공격기술 수행 이전에 수행한다)이다.

세 번째로 높은 우선순위(3)를 갖는 전술은 지속 유지(공격자가 APT 공격 과정에서 피해자 호스트 및 네트워크에서 장악력을 유지하기 위한 다양한 활동을 수행한다) 및 권한 상승(권한 상승을 통해 더 높은 권한을 획득한 행위 자체는 공격의 궁극적인 목표를 달성한 것은 아니지만 잠재적으로 공격 목표를 달성할 수 있는 다양한 행동을 수행할 수 있다)이다.

가장 낮은 우선순위(6)를 갖는 전술은 공격자가 피해자 호스트 또는 네트워크에 최초 침투하기 이전의 활동인 정찰 및 자원 개발 전술로, 지금은 폐기된 PRE-ATT&CK 프레임워크에 속한 전술 및 공격기술에 해당한다. 이와 대비하여 기본 우선순위(5)를 갖는 전술은 공격자가 피해자 호스트 또는 네트워크에 최초 침투하는 초기 접근 전술이다.

이를 제외한 실행, 방어 회피, 발견, 명령 제어 전술은 네 번째로 높은 우선순위(4)를 갖는다. 특히 방어 회피와 명령 제어 전술은 Technical Cyber Threat Framework의 진행 중 프로세스(ongoing process) 단계로 구분되어, 사이버 공격이 진행되는 단계 중간에 언제든지 수행될 수 있음을 나타낸다.

이를 바탕으로 전술에 대한 우선순위와 그에 따른 가중치는 Table 15.와 같이 부여하였다. 가장 높은 우선순위(1)부터 기본 우선순위(5)에 대해 각 가중치는 [1, 2] 범위 내에서 같은 간격으로 부여하고, 기본 우선순위 이하의 가장 낮은 우선순위(6)는 본격적인 침투 이전에 수행되는 행위이므로 1보다는 낮으나 동일한 간격(0.25)을 둔 0.75로 가중치를 부여하였다.

Table 15. Priority and corresponding weight of tactics

Tactic ID	Tactic Name	Priority	Weight
TA0042	Reconnaissance	6	0.75
TA0043	Resource Development	6	0.75
TA0001	Initial Access	5	1
TA0002	Execution	4	1.25
TA0003	Persistence	3	1.5
TA0004	Privilege Escalation	3	1.5
TA0005	Defense Evasion	4	1.25
TA0006	Credential Access	2	1.75
TA0007	Discovery	4	1.25
TA0008	Lateral Movement	2	1.75
TA0009	Collection	2	1.75
TA0010	Exfiltration	1	2
TA0011	Command and Control	4	1.25
TA0040	Impact	1	2

3.3.2 단위 공격기술 스코어링

3.2장의 9개의 요소와 전술 가중치를 이용하여 다음의 식 (7)에 따라 전술에 대한 가중치를 반영한 단위 공격기술의 스코어를 계산한다.

$$score_{\text{technique}} = w_{\text{tactic}} \times \frac{\sum_i score_i}{n} \quad (7)$$

여기서 w_{tactic}는 해당 공격기술이 속한 전술의 가중치, i는 3.2장의 각 요소, $score_i$는 요소별 점수를 의미한다. n은 Table 5.의 가장 마지막 열에 나열된 전술별 수치화에 고려되는 요소들의 개수 중 0점이 아닌 점수가 부여된 요소들(단, 절차 사례 요소는 0점을 포함)의 개수이다. 예를 들어, 다른 모든 고려 요소에 0점이 아닌 점수가 부여되었으나 CAPEC 공격패턴의 일반적 심각도에 대한 값이 부여되지 않은 공격기술에 대해서는 스코어링 요소에서 제외해야 하므로 분모가 n이 아닌 $n-1$이 된다. 식 (7)에 따른 점수는 $[0, 5]$점 범위 내에 분포한다.

Table 16.은 식 (7)에 따라 단위 공격기술에 대한 스코어를 산출하였을 때 전술별 통계 분포를 나타낸다. 전술의 후반부로 갈수록 스코어의 평균, 중간값을 포함한 전반적인 스코어 분포가 상승하는 경향이 있음을 확인할 수 있다.

Table 17.은 식 (7)에 따른 공격 스코어를 산출하였을 때 가장 높은 공격 스코어를 갖는 상위 20개의 공격기술을 나열한 것이다. 전술별로는 유출(6개), 영향(4개), 내부 확산(4개), 수집(3개), 자격증명 접근(2개), 권한 상승(1개)의 분포를 보이며, APT 공격의 후반 단계에서 수행되는 공격기술에 대해 높은 스코어가 부여됨을 확인할 수 있다.

Table 18.은 식 (7)에 따른 공격 스코어를 산출

Table 16. Statistics of score for individual (sub-)technique by tactics

Tactics	Min	Max	Average	Standard Deviation	Median	Q1	Q3	IQR	Lower Bound	Upper Bound
Reconnaissance	0.000	2.267	0.382	0.622	0.112	0.000	0.431	0.431	0.000	1.077
Resource Development	0.000	2.250	1.026	0.751	1.002	0.431	1.875	1.444	0.000	4.041
Initial Access	1.597	3.333	2.511	0.460	2.525	2.155	2.836	0.681	1.133	3.857
Execution	1.037	3.750	2.633	0.753	2.895	2.177	3.250	1.073	0.567	4.860
Persistence	1.245	5.049	2.639	0.941	2.495	1.852	3.300	1.448	0.000	5.472
Privilege Escalation	1.500	5.400	2.669	0.862	2.642	2.100	3.214	1.114	0.429	4.886
Defense Evasion	1.000	5.100	2.409	0.870	2.301	1.757	2.877	1.120	0.078	4.556
Credential Access	1.400	5.250	3.391	0.978	3.500	2.852	4.162	1.309	0.888	6.126
Discovery	1.000	4.063	2.579	0.703	2.549	2.145	3.125	0.980	0.674	4.595
Latetal Movement	2.063	6.054	4.184	1.014	4.247	3.500	4.916	1.416	1.376	7.039
Collection	1.400	5.250	3.742	1.149	3.720	2.891	4.699	1.807	0.180	7.410
Exfiltration	1.500	7.333	4.785	1.344	4.299	4.000	5.891	1.891	1.164	8.726
Command and Control	2.687	5.000	3.664	0.586	3.661	3.213	4.103	0.891	1.877	5.439
Impact	3.500	7.319	4.429	0.814	4.159	4.000	4.612	0.612	3.082	5.530

Table 17. Top 20 ATT&CK (sub-)techniques with high threat score

Tactic	Technique ID	Technique Name	Threat Score
Exfiltration	T1041	Exfiltration Over C2 Channel	7.333333333
Impact	T1495	Firmware Corruption	7.319402985
Exfiltration	T1029	Scheduled Transfer	6.626865672
Exfiltration	T1030	Data Transfer Size Limits	6.328358209
Exfiltration	T1048.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	6.288557214
Lateral Movement	T1550.004	Use Alternate Authentication Material: Web Session Cookie	6.054477612
Impact	T1486	Data Encrypted for Impact	6
Exfiltration	T1020	Automated Exfiltration	5.890547264
Lateral Movement	T1550	Use Alternate Authentication Material	5.818097015
Privilege Escalation	T1055	Process Injection	5.4
Impact	T1489	Service Stop	5.365671642
Impact	T1490	Inhibit System Recovery	5.365671642
Exfiltration	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	5.293532338
Lateral Movement	T1550.002	Use Alternate Authentication Material: Pass the Hash	5.281343284
Credential Access	T1056.001	Input Capture: Keylogging	5.25
Credential Access	T1056.003	Input Capture: Web Portal Capture	5.25
Lateral Movement	T1563	Remote Service Session Hijacking	5.25
Collection	T1005	Data from Local System	5.25
Collection	T1056.001	Input Capture: Keylogging	5.25
Collection	T1056.003	Input Capture: Web Portal Capture	5.25

Table 18. Top 20 ATT&CK (sub-)techniques with low threat score

Tactic	Technique ID	Technique Name	Threat Score
Reconnaissance	T1590	Gather Victim Network Information	0.111940299
Reconnaissance	T1590.001	Gather Victim Network Information: Domain Properties	0.111940299
Reconnaissance	T1591.002	Gather Victim Org Information: Business Relationships	0.111940299
Reconnaissance	T1593	Search Open Websites/Domains	0.111940299
Reconnaissance	T1593.001	Search Open Websites/Domains: Social Media	0.111940299
Resource Development	T1588.006	Obtain Capabilities: Vulnerabilities	0.111940299
Reconnaissance	T1589	Gather Victim Identity Information	0.223880597
Reconnaissance	T1589.003	Gather Victim Identity Information: Employee Names	0.223880597
Reconnaissance	T1590.005	Gather Victim Network Information: IP Addresses	0.223880597
Reconnaissance	T1592	Gather Victim Host Information	0.375
Reconnaissance	T1592.001	Gather Victim Host Information: Hardware	0.375
Resource Development	T1608	Stage Capabilities	0.375
Resource Development	T1608.003	Stage Capabilities: Install Digital Certificate	0.375
Reconnaissance	T1592.004	Gather Victim Host Information: Client Configurations	0.430970149
Reconnaissance	T1595.001	Active Scanning: Scanning IP Blocks	0.430970149
Resource Development	T1584.006	Compromise Infrastructure: Web Services	0.430970149
Resource Development	T1608.002	Stage Capabilities: Upload Tool	0.430970149
Resource Development	T1608.005	Stage Capabilities: Link Target	0.430970149
Reconnaissance	T1589.001	Gather Victim Identity Information: Credentials	0.447761194
Resource Development	T1586.002	Compromise Accounts: Email Accounts	0.447761194

하였을 때 0점을 제외한 가장 낮은 공격 스코어를 갖는 하위 20개의 공격기술을 나열한 것이다. 0점에 해당하는 공격기술들은 전술별로 정찰(19개), 자원 개발(5개)의 분포를 보였다. Table 18.에 나타난 공격기술에 대해 전술별로는 정찰(13개), 자원 개발(7개)의 분포를 보이며, APT 공격의 전반 단계에서 수행되는 공격기술에 대해 낮은 스코어가 부여됨을 확인할 수 있다.

3.4 전체 공격 스코어링

기존 연구[1, 2]에서는 전체 공격에 대한 스코어를 계산하기 위하여 전체 공격을 구성하는 각 단계의 공격 스코어를 곱하였다. HOLMES[1]의 경우 최대 $\prod_{i=1}^{7} 10^{\frac{10+i}{10}} = 6{,}309{,}573{,}445$(여기서 i는 록히드 마틴 社의 사이버 킬체인 모델[3]의 각 공격 단계), Hassan 등의 연구[2]에서는 $\prod_{i=1}^{n} 15$(n은 공격을 구성하는 공격 체인의 최대 길이)로, 공격을 구성하는 공격기술의 수가 많아질수록 전체 공격에 대한 스코어의 변화 폭이 매우 커지게 된다.

이와는 달리, 본 연구에서는 다음의 식 (8)과 같이 전체 공격을 구성하는 단위 공격기술의 공격 스코어를 더하여 전체 공격에 대한 스코어를 계산한다. 그 이유로 첫째, Table 16. 및 Table 18.에서 확인할 수 있듯이, 1보다 낮은 스코어를 가지는 공격기술이 존재하므로, 전체 공격에 대한 스코어를 산출할 때 단위 공격기술의 스코어를 곱하게 되면 해당 공격기술이 추가될 때 공격기술이 더 사용되었음에도 전체 스코어가 낮아지게 된다. 둘째, 전체 공격에 대한 스코어를 산출할 때 단위 공격기술의 스코어를 곱하게 되면 중간 정도의 스코어(2점 내외)를 가지는 공격기술을 다수 사용한 전체 공격의 스코어가, 매우 높은 스코어(4점 이상)를 가지는 공격기술을 소수 사용했을 때보다 스코어보다 높게 나오는 현상이 발생한다.

$$score_{\mathrm{APT}} = \sum_{k} score_{k} \tag{8}$$

여기서 k는 APT 공격을 구성하는 단위 공격기술이며, $score_k$는 각 공격기술의 스코어를 의미한다. 전체 APT 공격 관점에서 각 공격기술이 추가될 때마다 해당 공격기술의 스코어가 더해지면서 전체 공격에 대한 스코어가 증가하며, 따라서 HOLMES[1]와는 달리 Hassan 등의 연구[2]와 마찬가지로 스코어의 상한선이 존재하지 않는다.

IV. APT 공격 사례 스코어링

4장에서는 전 세계에서 발생하였던 APT 공격 사례를 분석하여 발표한 보고서에 ATT&CK 공격기술을 태깅하고, APT 공격 사례에 대한 공격 스코어

링을 수행한 결과를 제시한다.

4.1 데이터

여러 정부 기관, 기업, 연구소 등에서는 지금까지 전 세계에서 발생하였던 다양한 APT 공격을 분석하고 보고서의 형태로 공개하고 있다. APT & Cybercriminals Campaign Collection(CCC)[11]은 이들 보고서를 모아 연도별, 일자별로 분류해 놓은 저장소(repository)이다.

한편, rcATT(Reports Classification by Adversarial Tactics and Techniques)[12, 13]는 사이버 공격에 대한 분석 보고서에 ATT&CK의 전술과 공격기술을 태깅하는 도구로, 공격자가 APT 공격에서 수행한 공격기법에 대해 보고서에서 텍스트 형태로 서술한 내용을 가장 적합한 전술 및 공격기술을 찾아 이를 태깅한다. 본 연구에서는 CCC에서 수집한 APT 분석 보고서에 대해 rcATT를 이용하여 ATT&CK 전술 및 공격기술을 태깅하였고, 그 결과 CCC에 있는 1,086개의 보고서 중 957개에 공격기술이 태깅되었다.

4.2 분석 결과

rcATT를 이용하여 ATT&CK 공격기술을 태깅한 CCC의 APT 공격 보고서에 대해 3장의 공격 스코어링을 적용하였을 때, Table 19.와 같은 통계량을 나타내었다. Table 20.은 APT 공격 보고서에 대한 공격 스코어의 분포(왼쪽) 및 태깅된 ATT&CK 공격기술 개수의 분포(오른쪽)를 나타낸다. 특히 APT 공격 보고서에 태깅된 ATT&CK 공격기술은 10개 이하인 경우가 전체의 40.44%(387개 보고서)로 나타나, APT 공격 사례를 분석한 보고서는 전체 APT 공격 중 극히 일부에 대해 분석한 것으로 파악된다.

Table 21.[1]은 높은 공격 스코어를 갖는 20개의 APT 공격 사례들을 나열한 것이다. 가장 높은 공격 스코어를 갖는 APT 공격은 'Icefog'라는 공격 그룹(threat group)에 의해 수행된 'Icefog'라고 명명된 APT 공격 작전(operation)으로, 전술별로는 수집(8개), 명령 제어(7개), 자격증명 접근(1개), 방어 회피(10개), 발견(8개), 권한 상승(6개), 실행(7개), 지속 유지(3개), 내부 확산(2개)의 분포를 보인다. 또한 전반적으로 APT 보고서에서 공격기술이 많이 태깅될수록 높은 공격 스코어가 산출되는 것을 확인할 수 있었다.

공격 그룹[14]이 추정된(attributed) APT 공격 보고서에 대해, 주요 국가와 연관된 공격 그룹별 APT 공격 스코어를 Table 22.와 같이 분석할 수

Table 19. Statistics of threat score and number of techniques for APT threat reports

	Threat Score	Number of Techniques
Max	256.693	75
Min	1.521	1
Median	51.356	15
Average	23.7369284	17.342
Standard Deviation	19.18298317	13.387

Table 20. Histogram of (left) the entire threat score and (right) the number of (sub-)techniques tagged by rcATT[13] for APT reports in CCC[11]

Score	Number of Reports
1	51
2	61
3	44
4	63
5	62
10	228
20	342
30	262
40	195
50	105
60	76
70	68
80	59
90	42
100	46
110	48
120	46
130	26
140	28
150	18
200	37
250	5
300	2

# of (sub-) techniques	Number of Reports
1	51
2	57
3	33
4	34
5	44
6	42
7	37
8	26
9	41
10	22
15	100
20	125
25	89
30	83
35	69
40	49
45	26
50	15
60	9
70	3
80	2

1) Table 21.의 Operation 항목은 데이터셋의 보고서에서 APT 공격을 명명한 작전(operation) 항목이며, 보고서에서 APT 공격의 작전 항목이 정의되어 있지 않으면 'unidentified'으로 라벨링하였으며, unidentified_ 뒤에 명명된 숫자는 데이터 분석의 편의상 저자가 붙인 것이다.

Table 21. Top 20 ATP operations with high threat score

Operations	Threat Group	Threat Score	Number of Techniques	Average Threat Score for each (sub-)technique
Icefog	Icefog	256.693	75	3.423
unidentified_1039	APT32	252.675	70	3.610
Wocao	APT20	244.610	66	3.706
From Kill Chain to Ransomware	NaN	239.520	73	3.281
Machete	Machete	217.293	56	3.880
target diplomatic and government agencies, businesses	Patchwork	213.930	60	3.565
unidentified_964	Dragonfly	204.962	62	3.306
NAIKON - Traces from a Military Cyber-Espionage Operation	Naikon	193.392	51	3.792
Grandoreiro: How engorged can an EXE get?	NaN	189.727	56	3.388
Mofang	Mofang	189.311	52	3.641
Global Energy Cyberattacks Night Dragon	Night Dragon	188.593	53	3.558
The Operation GhostShell campaign	MalKamak	187.777	50	3.756
DRBControl	NaN	184.835	53	3.487
Spalax	NaN	181.018	51	3.549
El_Machete	NaN	178.734	47	3.803
Targets Air-gapped Environments	Tropic Trooper	177.043	50	3.541
targets japanese businesses	BRONZE BUTLER	175.428	46	3.814
target a global corporation based in Asia	APT32,Cobalt Kitty	175.246	55	3.186
Attack on Indian Government Financial Institutions	NaN	172.699	49	3.524
FIN8 Returns with Improved BADHATCH Toolkit	FIN8	171.241	48	3.568

Table 22. Average threat score of some threat groups associated with countries

Country	Threat Actor	Num. of Report	Average Threat Score	Num. of Tech.
North Korea	Lazarus Group	32	70.024	19.654
	Kimsuky	4	108.958	30.5
	Andariel	1	17.521	8
	APT37	8	86.592	24.250
	APT38	1	104.058	28
	(summary)	46	66.756	18.761
China	APT12	3	86.499	24.667
	APT17	1	10.468	4
	APT3	6	60.764	17.4
	Chimera	1	102.296	28
	Ke3chang	7	98.567	27.667
	Mofang	1	189.311	52
	Night Dragon	2	188.593	53
	APT20	1	244.610	66
	(summary)	22	99.473	27.895
Russia	APT28	34	48.642	13.9
	APT29	15	83	24.417
	Dragonfly	11	84.242	24.1
	Gamaredon Group	4	95.877	29.25
	Inception	1	56.569	17
	Nomadic Octopus	1	104.173	29
	Sandworm Team	14	84.694	23.5
	Turla	20	80.128	23.111
	(summary)	100	71.293	20.523

있었다. 북한으로 추정되는 공격 그룹과 관련한 APT 공격 사례(총 46건의 보고서)에 대해 평균 66.756점의 스코어가, 중국으로 추정되는 공격 그룹과 관련한 APT 공격 사례(총 22건의 보고서)에 대해 평균 99.473점의 스코어가, 러시아로 추정되는 공격 그룹과 관련한 APT 공격 사례(총 100건의 보고서)에 대해 평균 71.293점의 스코어가 산출되었다. 주의해야 할 점은 단순히 점수만을 비교하는 것이 아니라, APT 공격이 진행된 정도가 반영된 공격 기술의 수를 고려해야 한다. 이 때 APT 공격 사례에 대한 평균 스코어(공격 사례에 대한 전체 스코어를 태깅된 공격기술 수로 나눈 값에 대해, 해당 공격 그룹으로 특정된 국가에 대한 전체 평균)를 기준으로 북한(3.567), 중국(3.468), 러시아(3.457) 순으로 나타났다.

4.3 논의

먼저, APT 공격 사례 보고서는 작성자인 조직 또는 개인의 관심 성향에 따라 (1) APT 공격 과정 전체를 포함하거나, (2) APT 공격 과정에서 사용된 악성코드를 분석한 결과를 제시하거나, 또는 (3) 특정 APT 공격 사례가 아닌 특정 공격 그룹이 수행한

것으로 추정된 여러 APT 공격 사례를 종합하여 분석한 결과를 제시한다. 따라서 내용에 따라 포함될 수 있는 ATT&CK 공격기술의 범위와 항목이 달라질 수 있으며, 이에 따른 스코어 산출 결과가 APT 공격 사례 보고서에서 다루는 APT 공격을 숫자 그대로 받아들이기엔 어려움이 있다. 만약 APT 공격 사례 보고서에 대한 스코어를 비교하기 위해서는 보고서가 다루는 공격의 범위에 따라 분류하고 그들끼리 비교하는 것이 더 적절할 것으로 판단된다.

다음으로, APT 공격 사례 보고서는 인간이 읽을 수 있는(human-readable) 텍스트 형태로 작성되어 있으므로 특정 공격 방법을 암시하는 문구에 대한 ATT&CK 공격기술로의 태깅은 rcATT에서 자연어 처리와 머신러닝을 이용한 학습 및 분류를 통해 이루어진다[13]. 따라서, 동일한 ATT&CK 공격기술에 대해 보고서 작성자마다 다른 표현 방법을 사용하는 점, 아무리 좋은 머신러닝 알고리즘을 적용하여도 100% 완벽한 분류가 어려운 점 등은 부정확한 ATT&CK 공격기술 태깅이라는 한계를 가질 수밖에 없다.

V. 결론 및 향후 연구

본 연구에서는 APT 공격을 탐지하고 대응하기 위한 과정으로 APT 공격을 스코어링하는 방법을 제안하였다. 이를 위하여 공격기술에 대한 사실상 표준 모델인 MITRE ATT&CK 프레임워크를 이용하였다. 먼저 ATT&CK에 정의된 공격기술을 구성하고 있는 여러 요소 중 정량화 가능한 요소를 식별하고, 해당 요소들을 분석하여 요소별 스코어링 방안을 도출하였다. 정량화 요소들과 공격기술이 속한 전술에 대한 가중치를 이용하여 각 공격기술의 스코어를 산출하였다. 나아가, 여러 공격기술로 구성된 전체 APT 공격의 스코어를 산출하는 방안을 제안하였다. 제안한 스코어링 방법을 APT 공격 사례들을 분석한 APT 공격 보고서에 적용함으로써, APT 공격을 포함한 다양한 사이버 공격의 위협 수준 및 시급성을 판단하기 위한 정량화 가능성을 제시하였다.

본 연구에서 제안한 공격 스코어링 방법의 개선 방향은 다음과 같다. 첫째, 스코어링을 위해 사용하는 요소가 가질 수 있는 정성적인 값으로부터 정량적인 값으로의 변환은 여전히 논쟁의 여지가 있다. 예를 들어, 공격기술이 속한 전술의 개수를 스코어링에 반영하였을 때 최대 5점까지 부여될 수 있음을 전제로 설계하였으나, ATT&CK 프레임워크를 분석한 결과 특정 공격기술(T1078, Valid Accounts 및 이의 세부 공격기술)은 최대 4개 전술에 속하는 것을 확인하였다. 이에 따라 전술 요소에 대한 점수는 최대 4점까지 부여된다. 또 다른 예는 데이터 소스 및 방어 우회와 같은 요소에서 종류와 종류별 방법들의 개수를 기준으로 스코어를 부여하는 방법에서, 종류의 개수와 세부 방법들의 개수와 같은 양적인 차이가 아닌 그 종류와 세부 방법의 경중을 고려하여 가중치를 반영할 여지가 있다고 판단된다.

둘째, 공격기술에서 스코어링을 산출하는 요소 중 값이 존재하지 않아 0점이 부여된 요소는 이를 제외하고 공격기술에 대한 스코어를 산정함으로써 0점이 부여되지 않는 요소를 가진 다른 공격기술과의 형평성을 맞추고자 하였다. 특히 요구 권한, CAPEC 심각도와 같은 요소에서 많이 발견되었는데, 이는 실제로 0점이 아닌 데이터 누락으로 인한 null 값(또는 missing value)이며, 이에 대해 데이터 사이언스, 머신러닝, 딥러닝 등 다양한 데이터 활용 분야에서 사용되는 null 값 처리 방법을 적용하여 보완할 여지가 있다고 판단된다.

셋째, 두 공격기술이 속한 전술의 우선순위에 따른 가중치의 산정 또한 심층적인 연구가 필요하다. HOLMES[1]의 경우 록히드 마틴 사의 사이버 킬 체인[3] 모델을 기준으로 순차적으로 진행된다고 판단하여 공격 단계의 진행 순서에 따라 가중치를 부여한다. 그러나, 실제 APT 공격을 수행하는 과정에서 공격자들은 공격 단계를 순차적으로 수행하지 않고 공격자들의 목표 달성을 위해 일부 공격 단계를 건너뛰거나 상대적으로 후반 단계의 공격 단계를 먼저 수행할 수 있다. 그렇지만 여전히 각 공격 단계별로 경중의 차이가 있으며, 이를 세부적으로 고려한 전술의 우선순위 산정 및 이에 따른 가중치의 산정 과정이 보완될 여지가 있다.

현재 본 연구에서 제안한 스코어링 방법과 연계하여, APT 공격탐지 시스템[15]에서 탐지한 시점에 현재까지 진행된 공격 과정이 실제 공격인지 여부를 판단하기 위한 임계치(threshold)의 설정에 관한 연구를 진행하고 있다. 이를 통하여 탐지 시스템에서 (1) 탐지 시점에서 현재까지 진행된 것으로 간주되는 APT 공격에 대한 스코어를 산출하여 실제 APT 공격 여부를 판단하고, (2) 실제 APT 공격인 것으로 판단되는 경우 스코어를 기반으로 공격의 우선순위를 산정할 수 있다. 향후 APT 공격탐지 시스템과

연계된 호스트 및 네트워크 기반 공격 대응 시스템을 이용하여 시급하고 중요한 사이버 공격에 우선하여 대응할 수 있을 것이다.

References

[1] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar and V. N. Venkatakrishnan, "HOLMES: Real-time APT detection through correlation of suspicious information flows," 2019 IEEE Symposium on Security and Privacy, pp. 1137-1152, May 2019

[2] Wajih Ul Hassan, Adam Bates and Daniel Marino, "Tactical provenance analysis of endpoint detection and response systems," 2020 IEEE Symposium on Security and Privacy, pp.1172-1189, May 2020

[3] Eric M. Hutchins, 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, vol. 1, no. 1, pp. 80, 2011

[4] Sangsoo Kim, Shinwoo Shim, Seonyeong Lim and Seongmo Koo, "A Threat Prioritization Method Using User Behavior Data for Cyber Threat Hunting," The Journal of Korean Institute of Information Sciences, vol. 46, no. 11, pp.1853-1861, Nov. 2021

[5] Seokho Kim, Incheol Shin and Jaeki Jeong, "Personality Traits and Response Styles," The Journal of Survey Research, vol. 12, no. 5, pp.51-76, Jul. 2011

[6] Blake E. Strom et al., "MITRE ATT&CK: Design and Philosophy," Technical Report, Mar. 2020 (available at https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf)

[7] MITRE ATT&CK, https://attack.mitre.org/, accessed on Apr. 2022

[8] MITRE CAPEC, https://capec.mitre.org/, accessed on Apr. 2022

[9] SigmaHQ, Sigma, https://github.com/SigmaHQ/ sigma, accessed on April 2022

[10] NSA/CSS Technical Cyber Threat Framework v2, https://nsa.gov/portal/75/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf, accessed on Apr. 2022

[11] APT & CyberCriminal Campaign Collections, https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections, accessed on Apr. 2022

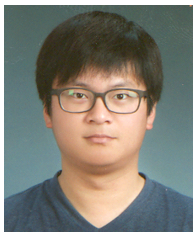
[12] vlegoy, rcATT, https://github.com/vlegoy/rcATT, accessed on Apr. 2022

[13] Valentine Solange Marin Legoy, "Retrieving ATT&CK tactics and techniques in cyber threat reports," MS thesis, University of Twente, 2019

[14] MITRE ATT&CK, Groups, https://attack.mitre.org/groups/, accessed on Apr. 2022

[15] Sungyoung Cho, Yongwoo Park and Kyeongsik Lee, "Implementation of an APT attack detection system through ATT&CK-based attack chain reconstruction," Journal of The Korea Institute of Information Security and Cryptology, vol. 32, no. 3, pp. 527-545, Jun. 2022

〈저 자 소 개〉



조 성 영 (Sungyoung Cho) 정회원
2009년 8월: 한국과학기술원 정보통신공학과 학사
2013년 2월: 한국과학기술원 정보보호대학원 석사
2013년 9월~현재: 국방과학연구소 사이버/네트워크 기술센터 선임연구원
〈관심분야〉 정보보호, 사이버 상황인식, 사이버 보안 시각화, 사이버전

박 용 우 (Yongwoo Park) 정회원
2018년 2월: 고려대학교 사이버국방학과 학사
2018년 8월~현재: 국방과학연구소 사이버/네트워크 기술센터 현역연구원
〈관심분야〉 정보보호, 사이버 보안 시각화, 사이버전

이 건 호 (Kunho Lee) 정회원
2017년 2월: 고려대학교 사이버국방학과 학사
2017년 8월~현재: 국방과학연구소 사이버/네트워크 기술센터 현역연구원
〈관심분야〉 정보보호, 사이버전, 암호

최 창 희 (Changhee Choi) 정회원
2008년 2월: 연세대학교 컴퓨터과학과 학사
2010년 2월: 한국과학기술원 전산학과 석사
2013년 8월: 한국과학기술원 전산학과 박사
2013년 9월~현재: 국방과학연구소 사이버/네트워크 기술센터 선임연구원
〈관심분야〉 정보보호, 사이버전, 머신러닝 기반 사이버 보안, AI, GAN

신 찬 호 (Chanho Shin) 정회원
2018년 2월: 고려대학교 사이버국방학과 학사
2018년 8월~현재: 국방과학연구소 사이버/네트워크 기술센터 현역연구원
〈관심분야〉 정보보호, 인공지능

이 경 식 (Kyeongsik Lee) 정회원
2009년 2월: 세종대학교 컴퓨터공학과 학사
2011년 2월: 고려대학교 정보경영공학과 석사
2011년 1월~현재: 국방과학연구소 사이버/네트워크 기술센터 선임연구원
〈관심분야〉 정보보호, 디지털 포렌식, 침해사고대응