



2023년 한국정보보호학회 하계학술대회

CISC-S'23

Conference on Information Security and
Cryptography Summer 2023

2023년 6월 22일(목)~23일(금)

강원대학교 춘천캠퍼스 60주년 기념관

주최



한국정보보호학회
Korea Institute of Information Security & Cryptology

주관



KNU 강원대학교
KANGWON NATIONAL UNIVERSITY

후원



국가정보원
NATIONAL INTELLIGENCE SERVICE



과학기술정보통신부



행정안전부



한국인터넷진흥원

ETRI

한국전자통신연구원
Electronics and Telecommunications
Research Institute

NSR

국가보안기술연구소
National Security Research Institute

Google

2023년 한국정보보호학회 하계학술대회 CISC-S'23

Conference on Information Security and Cryptography Summer 2023

시간/세션	발표 논문	페이지
10:50~12:20 암호 및 부채널 분석 4 좌장 : 박명서 (강남대학교)	SIDH 공격이 아이소제니 기반 암호에 미치는 영향 분석 허동희(고려대학교), 김수리(성신여자대학교), 홍석희(고려대학교)	514
	RISC-V 환경에서 CRYSTALS-Dilithium의 Montgomery Reduction 및 Butterfly 연산 최적 구현 최용렬, 김영범, 서석충(국민대학교)	518
	AIMer 전자서명 내부의 AIM 대칭 프리미티브 고속 구현 이민우, 장경배, 권혁동, 심민주, 송경주, 서화정(한성대학교)	522
	PIPO에 대한 차분 및 차분 중간일치 공격 김인성, 신한범, 김선엽, 권동근, 김선규, 신명수, 이동재(고려대학교), 김성겸(삼성전자), 홍득조(전북대학교), 성재철(서울시립대학교), 홍석희(고려대학교)	527
	TTA 표준 양자내성암호 HiMQ 안전성 분석 조성민, 서승현(한양대학교)	531
	KpqC 1라운드 SMAUG에 대한 개인키 복구 부채널 공격 이정환, 김규상, 김희석, 홍석희(고려대학교)	535
09:00~10:30 디지털 포렌식 좌장 : 김준섭 (고려대학교)	시그널 아티팩트 분석을 통한 디지털 수사에서의 활용 위다빈, 이신영, 박명서(강남대학교)	539
	MITRE ATT&CK Matrix 연계 사이버 공격 도구 프로파일링을 위한 표식체계 연구 유정현, 김영서, 이가영, 주근영, 하태주(세종대학교) 김원철(국방부), 이세한, 박기웅(세종대학교)	543
	전자파 분석을 통한 하드웨어 지갑 키 추출 박동준, 최민식, 김규상, 배대현, 김희석, 홍석희(고려대학교)	547
	메신저 포렌식 관점에서의 웹 아티팩트 분석 : 디스크드를 중심으로 이수미, 유지원, 박지원, 김성민(성신여자대학교)	551
	안티 디버깅 기술/무력화 연계분석을 통한 우회 프레임워크 설계 최기상, 최상훈, 박기웅(세종대학교)	555
	디지털 포렌식을 위한 스마트 홈 플랫폼 아티팩트 수집 및 식별 방안 김유빈, 신동혁, 엄익채(전남대학교)	559
09:00~10:30 시스템 보안 3 좌장 : 이새움 (한국인터넷진흥원)	최신 안티 퍼징 동향 분석 전일신, 정지우, 황은비, 권태경(연세대학교)	563
	제로트러스트 성숙도 모델 분석 및 제안 양경아(국가보안기술연구소), 광송이(송실대학교), 오형근, 박기태(국가보안기술연구소), 정수환(송실대학교), 박정수(호서대학교)	567
	개방형 OS 개발 라이프 사이클을 고려한 SBOM 활용 연구 김이레, 이만희(한남대학교)	571
	미국 연방 정부의 안전한 소프트웨어 도입을 위한 자가 증명 양식 분석 양식 분석 유현아, 이만희(한남대학교)	575
	딥페이크 탐지 모델의 보편적 검증 데이터셋 구성을 위한 딥페이크 생성 기법 분석 연구 김현준, 박래현, 김재욱, 오명교, 박재우, 권태경(연세대학교)	579
	모바일 앱을 위한 블랙박스 기반 테스트 입력 자동 생성 기술 동향 김다영, 조효진(송실대학교)	583

MITRE ATT&CK Matrix 연계 사이버 공격 도구 프로파일링을 위한 표식체계 연구

유정현*, 김영서*, 이가영*, 주근영*, 하태주*, 김원철¹, 이세한², 박기웅[†]

, [†] 세종대학교 정보보호학과 (학부생, 교수[†])

¹ 대한민국 국방부 사이버작전사령부

² 세종대학교 시스템보안연구실 (지능형드론 융합전공) (대학원생)

A Study on Marker System for profiling Cyber Attack Tools linked to MITER ATT&CK Matrix

Jeong-Hyeon Yoo*, Young-Seo Kim*, Ga-Young Lee*, Geun-Yeong Ju*,
Tae-Ju Ha*, Won-Chul Kim¹, Se-Han Lee², Ki-Woong Park[†]

*, [†] Dept. of Computer and Information Security, Sejong University
(Undergraduate Student*, Professor[†])

¹ Cyber Operations Command, Ministry of National Defense

² SysCore Lab. (Convergence Engineering for Intelligent Drone),
Sejong University (Graduate Student)

요약

현대 사회에서 디지털 환경이 확장됨에 따라 사이버 공격 빈도가 증가하고 있다. 이러한 사이버 공격에는 다양한 공격 도구가 사용되고 있으며 공격 도구의 복잡성과 위험도 또한 증가한다. 그러나 증가하는 사이버 공격 빈도 추세와 달리 공격기법과 기술의 변화 폭은 크지 않다. 따라서 선제적으로 공격 도구의 특성과 기능을 파악하고 체계적인 기준을 통해 무기를 식별할 필요가 있다. 본 논문에서는 도구 식별을 위한 도구 프로파일링을 수행하고, 사이버 공격과 관련된 다양한 정보의 표준 모델인 MITRE ATT&CK Matrix와의 도구 연계를 위한 표식체계를 제안한다. 이를 통해, 공격 도구의 기능적 DNA를 파악과 체계적이고 효율적인 공격 분석과 대응 전략 수립을 지원할 수 있다. 또한, 공격자의 전술과 기술을 이해하고 방어 전략 강화가 가능하다.

I. 서론

현대의 디지털화된 환경에서 사이버 공격 빈도는 지속적으로 증가하고 있으며, 그 공격의 복잡성 또한 증대되고 있다[1]. 공격자들은 다양한 기술과 전략을 사용하여 시스템에 침투하고, 중요한 정보를 탈취하는 등의 악의적인 행위를 수행한다. 사이버 공격은 다양한 공격 도구를 활용하여 이루어지므로 이에 대응하기 위해서는 선제적으로 공격 도구의 특성과 기능을 파

악하고 무기를 식별할 필요성이 있다. 또한 증가하는 사이버 공격과 달리 공격기법과 기술은 이전에 비해 크게 바뀌지 않는 것으로 확인되었다. 실제로 구글 클라우드 맨디언트[2]는 작년 한 해 사이버 공격 그룹은 역대 최대로 증가했지만, 공격기법과 기술들은 비슷하다고 밝혔다[3]. 이러한 상황에서 공격 도구의 프로파일링을 통해 무기를 식별할 수 있다면 공격과 방어적 측면에 큰 도움이 될 것이다.

따라서 MITRE ATT&CK matrix를 기반으로 사이버 공격 도구의 특성을 분석한다. 이를 토대로 공격 도구와 MITRE ATT&CK matrix 연계를 위한 표식체계를 제안하고자 한다. 이는 공격자가 각 공격 전술 단계에 맞는 도구를 선택하고 해당 도구를 사용하여 효과적인 공격을

[†]교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신방송기술국계공동연구사업(Project No. RS-2022-00165794, 40%), 국방ICT융합사업(Project No. Project No.2022-0-00701, 10%), 실감콘텐츠핵심기술개발사업(Project No. RS-2023-00228996, 10%), 대학ICT연구센터 육성지원사업(Project No. 2023-2021-0-01816, 10%) 및 한국연구재단 개인기초연구과제(Project No. RS-2023-00208460, 30%)의 지원을 받아 수행된 연구임.

수행할 수 있도록 지원할 것이다.

본 연구의 중요성은 사이버 공격에 대한 이해와 대응 능력을 향상하는 데에 있으며, 연구자들은 이러한 표식체계를 활용하여 공격 도구의 선택과 활용에 대한 통찰력을 얻을 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 사이버 공격 도구와 MITRE ATT&CK 프레임워크 사이의 표식체계를 정의하고, 3장에서는 사이버 공격 도구 프로파일링 환경 구축을 진행한다. 4장에서는 사이버 공격 도구와 MITRE ATT&CK matrix의 연계 결과를 보여준다. 5장에서는 결론 및 해당 연구의 기대효과와 향후 연구계획에 관해 서술한다.

II. 프로파일링 표식체계 정의

MITRE ATT&CK과 관련된 앞선 연구[4]에서는 사이버 공격 그룹의 연계만을 다루었다. 따라서, 공격 도구의 특성과 연계되는 전술과 기술을 시각적으로 명확하게 파악할 수 있는 표식체계를 정의하고자 한다.

2.1 MITRE ATT&CK 프레임워크

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) 프레임워크[5]는 사이버 공격의 전술, 기술, 소프트웨어 등 공격과 관련된 다양한 정보의 표준 모델이다. 전 세계에서 발생하는 사이버 위협에 대응하기 위해 설계되었으며 효과적인 사이버 공격 대응을 지원한다.

2.2 프레임워크 연계 표식체계 정의

	RC Reconnaissance 10 techniques	RD Resource-Development 8 techniques	IA Initial Access 9 techniques	EX Execution 14 techniques	PR Persistence 19 techniques
1	Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)
2	Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs
3	Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)
4	Gather Victim Network Information (5)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)
5	Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions
6	Phishing for Information (3)	Establish Accounts (3)	Replication Through	Inter-Process	Compromise Client Software

그림 1. MITRE ATT&CK 연계 표식체계 예시

MITRE ATT&CK 전술 정보를 명확하게

표현하기 위해 각 tactic을 [표 1]과 같이 코드화하였다. 또한 [그림 1]과 같이 전술에 속하는 하위 기술에 번호를 부여함으로써 전술 기술에 대한 인텔싱이 가능한 Armoury Mark System for Linkage(이하 AML) 표식체계를 정립하였다. 본 정립에서 서로 같은 전술에 속하는 하위 기술들은 대괄호로 묶어 정의하였고 다른 전술에 속하는 경우 콜론으로 구분하여 각 전술을 구분하였다. 이를 통해 하위 기술들이 해당 전술의 하위 범주에 속한다는 의미를 명확하게 전달하였으며, 결과적으로 AML 표식체계를 이용한 공격 도구는 tool name - code[number]:code[number] 형식으로 표현된다.

CODE	MITRE ATT&CK Tactics
RC	Reconnaissance
RD	Resource Development
IA	Initial Access
EX	Execution
PR	Persistence
PE	Privilege Escalation
DE	Defense Evasion
CA	Credential Access
DI	Discovery
LM	Lateral Movement
CO	Collection
EXF	Exfiltration
C2	Command and Control
IM	Impact

표 1. MITRE ATT&CK Tactics 코드화

III. 프로파일링을 위한 환경 구축

본 논문에서는 공격 도구 프로파일링을 통해 MITRE ATT&CK 프레임워크와 연계를 위해 프로파일링 환경 구축을 진행하였다. 공격 도구 프로파일링 과정을 수행하기 위해서는 공격 도구가 실행되는 환경 및 가상의 공격 대상을 구축해야 한다. 따라서 각 공격 도구에 맞는 가상 머신의 운영체제 설치 후 네트워크 설정, 추가 소프트웨어 설치, 보안 설정을 진행하였다.

3.1 Nmap

Nmap[6]의 경우에는 [그림 2]와 같이 공격 서버의 Kali Linux, 공격 대상 서버의 Metasploitable2를 docker환경에서 tcpdump로 eth0 인터페이스를 경유하는 네트워크 패킷들을 분석하였다.

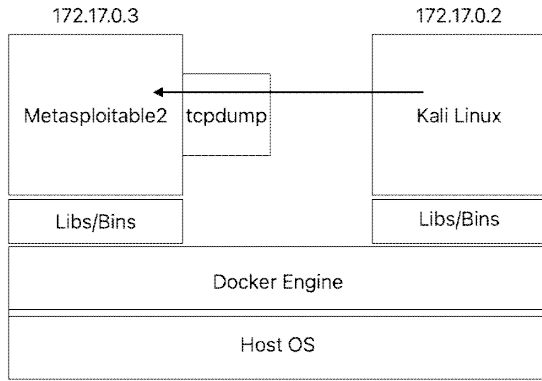


그림 2. 공격 도구 실행을 위한 도커 환경 예시

3.2 Burp Suite

Burp Suite[7]의 brute force 공격을 테스트 하기 위해 일반적인 웹 서버에 회원가입, 로그인 기능이 포함된 환경을 구축했다. 또한, 피해 서버는 사용자의 요청을 자동으로 기록하는 동작을 수행한다. Burp Suite의 proxy와 intruder 기능을 활용하여 피해 서버로 전송되는 패킷을 조작한 뒤, brute force 공격을 실행했다. 이를 통해 다양한 조합의 인증 정보를 시도하여 악의적인 접근을 시도하는 공격 시나리오를 구현하였다.

IV. 프로파일링 결과

4.1 프로파일링 기준

공격 도구에 대한 표식을 부여하기 위해 일차적으로 도구에 대한 기능 분석을 수행하였다. MITRE ATT&CK 프레임워크와의 긴밀한 연계를 위해 이차적으로 프레임워크 내의 tactics, techniques, data sources를 이용하였다. MITRE ATT&CK data sources는 여러 형태의 inspection data 종류 및 주제를 카테고리화한 데이터셋을 의미한다[5]. 침투된 피해 서버에 남아있는 로그 데이터나 센서 등이 그 예시이다.

MITRE ATT&CK 프레임워크의 tactics, techniques와 data sources와의 관계 구조는 [그림 3]과 같다.

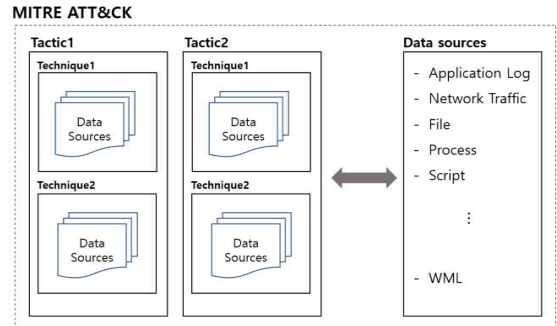


그림 3. MITRE ATT&CK 연계 데이터

기능 분석을 수행한 뒤 각각의 기능이 수행되었을 때 남는 공격자의 흔적과 연계하여 해당하는 data source를 선별했다. 선별한 data source로 techniques를 필터링하여 공격 도구의 기능과 연계된 technique을 도출한다. 도출된 technique을 통해 최종적인 무기 표식 코드를 표현할 수 있다.

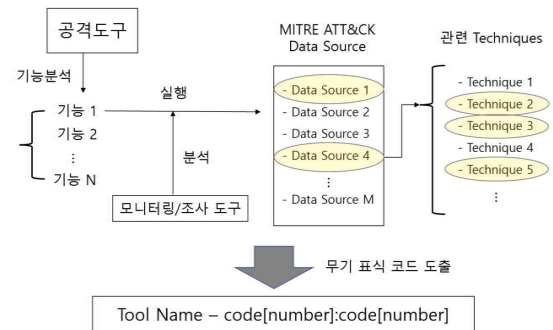


그림 4. 무기 표식 코드 도출

4.2 Case study: Nmap

공격 과정에서 필수적인 피해 대상 정보 수집 기능을 가지며 많은 옵션을 포함한 공격 도구 'Nmap'이 AML 표식체계의 효용성을 잘 보여줄 수 있어 대표 케이스 스터디 도구로 선정하였다. 본 연구를 위해 구축된 테스트베드 환경에서 Nmap 도구의 실제 실행을 통해 네트워크 스캐닝, 스크립트 스캐닝, 스푸핑, 운영체제 감지, 서비스 식별 등의 기능을 도출할 수 있다.

공격 서버에서 TCP 연결을 사용한 포트 스캐닝을 수행하였고, 공격 대상 서버에 TCPDump[8]를 사용하여 패킷을 캡처하였다. 이는 MITRE ATT&CK data source의 &Network Traffic&에 매핑할 수 있다. Network Traffic과 연계되며 Nmap과 관련 있는 technique으로 Active Scanning, Gather Victim Identity Information, Network Service Discovery, Remote System Discovery가 도출되었다.

이와 같은 방식을 사용하여 Nmap에 해당하는 data source로 Internet Scan, Command, Process, Script를 선별할 수 있다. 연계되는 technique으로 Gather Victim Host Information, Gather Victim Network Information, Network Service Discovery, Peripheral Device Discovery, Remote System Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Service Discovery가 도출된다.

최종적으로, 공격 도구 Nmap의 표식체계는 Nmap - RC[1,2,3,4,]:DI[14,18,22,24,26,27,29]로 정의할 수 있다.

V. 결론

현재 사이버 공격은 다양한 공격 도구가 활용되어 지속적으로 증가하고 있다. 공격 빈도와 피해 범위 또한 증가하는 현시점에서 선제적으로 무기 식별을 수행하여 대응할 필요가 있다. 따라서 본 논문에서는 MITRE ATT&CK matrix 기반 표식체계를 정의하고 공격 도구 프로파일링을 통한 MITRE ATT&CK techniques와의 매핑을 제안하였다.

다양한 공격 도구를 프로파일링하고 비교함으로써 유사성과 차이점을 도출할 수 있으며, 이를 통해 공격 도구의 기능적 DNA를 파악하고, 관련된 공격 도구들 사이의 관계를 분석할 수 있다. 결과적으로, AML 표식체계를 활용한 사이버 공격 도구의 매핑은 MITRE ATT&CK

matrix와의 연계를 가능하게 하여 더 체계적이고 효율적인 공격 분석과 대응 전략 수립을 지원할 수 있으며, 이를 통해 공격자의 전술과 기술을 이해하고 방어 전략을 강화하는 데 도움이 될 것이다.

향후 더 많은 사이버 공격 도구와 MITRE ATT&CK 프레임워크의 matrix 데이터를 수집하고 분석하여 AML 표식체계를 더욱 정교하게 확장하고자 한다. 또한 이를 통해 다양한 사이버 공격 도구에 대한 매핑 규칙과 특성을 탐색하고, 실제 사이버 공격 시나리오에 적용이 가능한 자동화된 분석 및 매핑 도구를 개발하고자 하며, 이러한 후속 연구를 통해 사이버 공격에 대한 이해와 대응 전략의 향상을 위한 중요한 기여가 가능할 것으로 기대된다. 자동화된 분석 및 매핑 도구를 활용하여 더욱 신속하고 정확한 사이버 공격 분석을 수행할 수 있고, 새로운 사이버 공격 기법 및 도구에 대한 식별과 대응이 가능해질 것으로 기대되며, 결과적으로 이는 사이버 보안 산업 전반에서 매우 유용한 도구로써 활용할 수 있다.

[참고문헌]

- [1] 윤민우, “사이버 안보위협 의 문제와 전략적 의미, 그리고 대응방안에 대한 연구”, 국가안보와 전략, 제14권 제4호, pp.111 - 147, 2014.12.
- [2] Google Cloud Mandiant, <https://www.mandiant.com/>
- [3] 이유지, “활동 중이 사이버공격그룹 역대 최다...공격기법 비슷, 기술도 재탕”, Byline Network, 2023.05.
- [4] 최창희, 신찬호, 신성욱, &MITRE ATT&CK 모델을 이용한 사이버 공격 그룹 분류&, 인터넷정보학회논문지, 제23권 제6호, pp.1-13, 2022.12.
- [5] MITRE ATT&CK, <https://attack.mitre.org/>
- [6] NMAP, <https://nmap.org/>
- [7] BURP SUITE, <https://portswigger.net/>
- [8] TCPDump, <https://www.tcpdump.org/>