사이버 공격 해킹 그룹 특성 분석 방법 연구

고명석*, 김지량*, 유도진**
*극동대학교 대학원 인공지능보안학과
**극동대학교 해킹보안학과
e-mail:dhy8906@naver.com

Research on cyber attack hacking group characteristics analysis method

Myung-Seok Ko*, Prof. Ji Ryang Kim*, Prof. Doh Jin Yoo**
*FarEast University Graduate School of Artificial Intelligence Security
**Dept. of Department of Hacking Security, FarEast University

요 약

본 논문은 PC 분야에서 발생한 침해사고에서 악성코드를 분석하고, 특정 시그니처를 사용하여 공격그룹들을 식별하는 과정을 넘어서, Mitre ATTACK 프레임워크를 효율적으로 활용하기 위한 방법론을 제안한다. 더 나아가, 북한 기반의 APT37 그룹에 속한 것으로 추정되는 공격사례와 Konni로 알려진 악성코드를 활용한 공격사례를 Mitre ATTACK 침해 지표로 분석하고, 이를 통해 두 공격사례 간의 유사성을 비교하여 공격 유사성을 확인할 수 있었다. 따라서, 이 연구는 두 공격사례 간의 관련성을 확인하는데 기여한다. 또한 악성코드 분석이 완료된 데이터의 정제 및 데이터베이스 구축을 통해 공격그룹 식별을 위한 환경 구성을 제안한다.

1. 서론

한국인터넷진흥원(이하, KISA)에서 발간하는 2023년 상반기 사이버 위협 동향 보고서 중 민간분야 침해사고 현황 통계에 따르면 2021년 640건에서 2022년 1,142건으로 전년 대비 약 2배가 증가하였으며, 2023년 상반기 침해사고 신고 건수는 664건으로 전년 상반기 대비 40% 증가하였다. 2021년부터 2023년까지 반기별 침해사고 신고 현황을 살펴보면 2021년 상반기 298건/ 하반기 342건, 2022년 상반기 473건/ 하반기 669건이며, 2023년 상반기엔 664건의 침해사고 신고가 있었다[1]. 침해사고 신고 유형 중 악성코드 감염 통계를 살펴보면 악성코드 감염 90% 이상의 비중을 랜섬웨어 신고가 차지하고 있었으며, 2022년 랜섬웨어 신고는 325건으로 지난 4년간 8.3배로 급속히 증가하였다. 2023년 상반기 랜섬웨어 침해사고 현황을 살펴보면 전년 상반기 대비 14% 증가한 134건인 것으로 나타났으며, 중견기업이 전년 대비 3배 증가한 17건, 중소기업도 12% 증가한 110건인 것으로 나타났다[1].

보안 분야의 기업과 국가기관은 침해사고 예방에 상당한 자금과 리소스를 집중하고 있음에도 불구하고, 침해 공격은 점차 다양한 형태들로 진화하고 있으며, 공격기법은 더욱 정교해지고 있다. 또한, 각 보안 관련 기업들과 국가기관은 발생한 침해사고들을 해결하기 위해 악성코드 분석 및 해킹그룹 식별에 큰 노력을 기울이고 있지만, 해킹그룹은 자신들을 드러내지 않는 특성으로 인해 공격 원점 파악에 어려움을 겪고 있다. 이에 본 연구에서는 침해사고 발생 시 Sysmon Modular를 사용한 Mitre ATTACK 침해 지표를 수집하고, 수집된 침해 지표를 활용하여 이전의 공격사례 침해 지표와의 비교 분석을 통해 공격 유사성을 식별하였다. 해당 결과를 토대로 해킹그룹 특정을 위한 방법론 및 해킹그룹의 특성을 나타내기 위한 분석 절차를 제시한다.

2. Mitre ATTACK

공격자들의 전략과 기법을 분석하고 체계화하기 위한 프레임워크인 “Mitre ATTACK (Adversarial Tactics, Techniques, and Common Knowledge)”은 실제 사이버 공격 사례를 관찰한 후 공격자가 사용한 악의적 행위(Adversary behaviors)에 대해서 공격 전술(Tactics)들과 기술(Techniques)의 관점으로 분석하여 다양한 공격그룹의 공격기법들에 대한 정보들을 분류해 목록화한 표준적인 데이터들이다. 2023년 8월 1일 기준 Mitre ATTACK v13.1이 공개되었다.

Mitre ATTACK은 전통적인 사이버 킬체인의 개념과는 차이점을 가지며, 지능화된 공격 탐지 향상을 위해 위협적인 전략과 기술을 체계화하고 패턴화하는 것이 특징이다. 초기 Mitre는 Windows 네트워크 환경에

대한 해킹 공격에 관한 전술(Tactics), 기술(Techniques), 절차(Procedures) 등 TTP(Tools, Techniques, Procedures)를 문서화하는 목적으로 시작되었으며, 이후 공격그룹으로부터 나오는 일관된 공격 행동 패턴을 분석하여 TTP 정보들을 매핑하고, 공격그룹의 활동을 식별하는 프레임워크로 발전한다.

아래[표 1]에서는 각 전술 단계별로 사용되는 상위기술들과 각 상위기술에 해당하는 하위기술 개수를 나타낸다.

[표 1] PC 분야 전술에 따른 상위공격 기술과 하위기술 개수

Mitre 전술 단계	상위기술	하위기술
정찰	10가지	33개
자원개발	8가지	37개
초기접근	9가지	10개
실행	14가지	22개
지속성 확보	19가지	97개
권한 상승	13가지	90개
탐지 회피	42가지	162개
인증 정보 획득	31가지	12개
발견	31가지	12개
공격 대상 이동	9가지	13개
수집	17가지	20개
명령 및 제어	16가지	23개
유출	9가지	9개
영향	13가지	13개

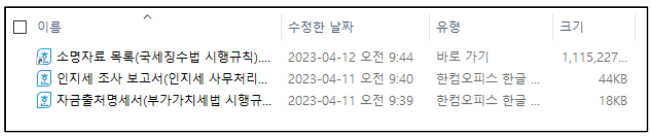
또한 각 전술 단계와 관련된 기술은 일반적으로 아래 [표 2]와 같이 고유한 ID로 정의된다. 정찰 단계는 TA0043으로 설정되며, 이러한 단계와 연결된 상위기술들 중 하나인 "Phishing for Information"은 T1598로 정의된다. 또한, 해당 상위기술에 대한 세부 기술로 "Spearphishing Service"가 T1598.001로 정의된다.

[표 2] 정찰 단계 중 상위기술 명칭과 하위기술 명칭

Mitre 전술 단계	상위기술	하위기술	하위기술 명칭
TA0043 정찰	T1598 (Phishing for Information)	T1598.001	Spearphishing Service

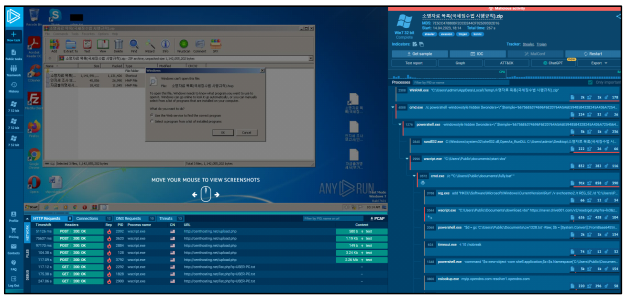
3. 분석 환경 구축

본 연구를 위해 분석 환경을 구축하며, 악성코드 샘플을 수집하였다. 아래 [그림 1]에 따르면, 악성코드는 Konni로 명명되며, 이는 2023년 7월 31일에 발생한 국세청 우편물 발송 알림 사칭 공격에 사용되었다. Konni는 주로 대북 분야 기업들을 대상으로 이메일 기반의 스피어 피싱 공격을 수행하며, 악성 파일은 '소명 자료 제출 요청 안내.zip'이라는 이름의 압축 파일로 첨부되었다. 압축 파일 내에는 2개의 HWP 문서 파일과 1개의 LNK 바로가기 파일이 포함되어 있으며, LNK 파일명은 '소명자료 목록(국세징수법 시행규칙).hwp.lnk'으로 확인되었다.

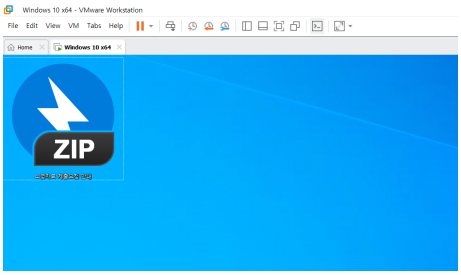


[그림 1] Konni 악성코드 샘플 파일

이어 [그림 2]에 따라 OSINT(Open Source Intelligence) 도구인 AnyRun을 활용하여 악성코드 샘플을 획득하였으며, [그림 3]에 나타난 바와 같이 VmWorkstation 17 Pro 가상화 소프트웨어를 사용하여 동적 분석을 수행하였다.



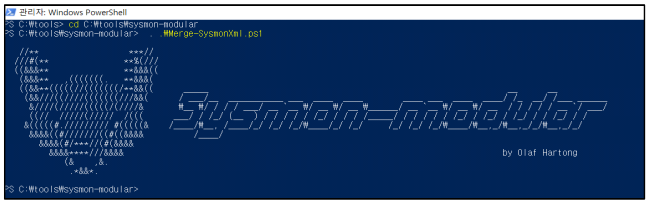
[그림 2] AnyRun을 활용한 악성코드 샘플 수집



[그림 3] VmWorkStation 17 가상화 환경

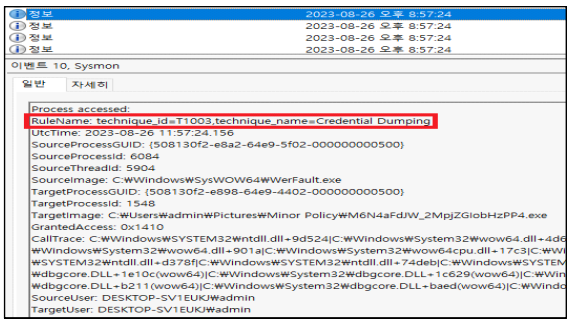
3.1 Sysmon Modular

동적 분석을 위해, Windows 환경에서 악성코드의 활동 로그를 기록하는 도구인 Sysmon을 활용하였다. Sysmon은 Windows 시스템의 다양한 활동을 Event ID로 기록하며, 각 Event ID는 서로 다른 유형의 활동을 나타낸다. 이러한 이벤트들은 로그 파일에 저장되며, Sysmon의 기능을 확장하기 위해 [그림 4]와 같이 GitHub에서 제공하는 Modular를 활용하였다.



[그림 4] Modular가 적용된 Sysmon

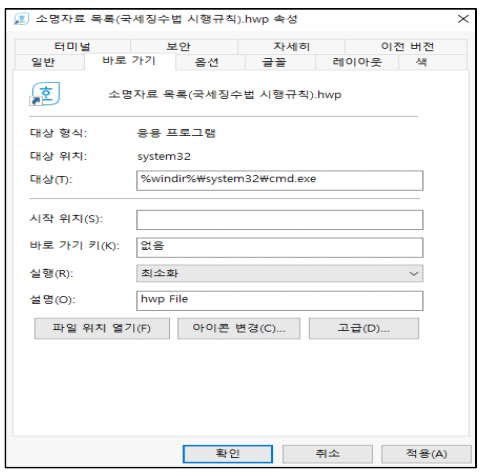
이를 통해, Windows 환경에서 악성 활동으로 판단되는 특정 활동에 아래 [그림 5]와 같이 Mitre ATT&CK Techniques 정보를 추가하여 침입 감지 지표를 생성하였다.



[그림 5] Modular가 적용된 Sysmon 로그 중 악성 로그 Mitre 정보

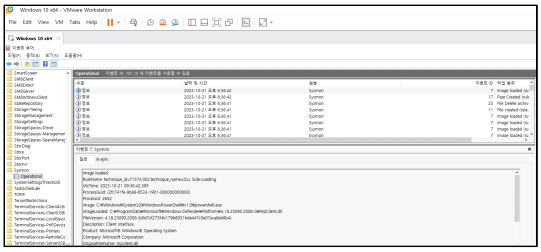
4. 악성코드 분석 진행

분석 환경을 구축한 후, 앞서 AnyRun을 통해 획득한 "소명자료 제출요청 안내.zip"으로 가장한 Konni 악성코드를 분석하였다. 해당 압축 파일 내부에는 총 3개의 파일이 존재하며, 그 중 2개는 HWP 한컴 오피스 문서이고, 나머지 하나는 아래 [그림 6]과 같이 HWP 문서처럼 가장한 2중 확장자의 LNK 파일이다. 해당 LNK 파일은 '%windir%\system32\cmd.exe' 명령과 함께 별도의 인자를 실행하도록 구성되어 있으나, Windows 화면상에는 표시되지 않는다.



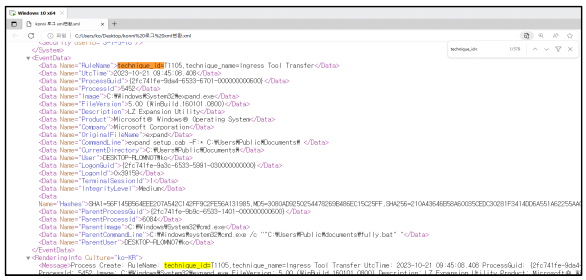
[그림 6] 한글파일로 가장한 소명자료 목록.LNK파일

LNK 파일 실행 시, 아래 [그림 7]과 같이 모듈러가 적용된 Sysmon은 10분 동안 444개의 로그를 기록하였으며, 이 중 악성 행위로 의심되는 로그에는 Mitre Technique 정보가 포함되어 있었다.



[그림 7] 악성코드 실행 시 발생한 Sysmon 이벤트 로그

발생한 로그 내용을 확인하기 위해 해당 로그를 XML파일 형식으로 저장한다. 저장된 로그 내용 중 아래 [그림 8]과 같이 텍스트 필터링 기능을 통해 Mitre Techniques과 관련된 로그를 확인할 수 있다.



[그림 8] xml 로그 파일 내 Mitre Techniques 검색

상기 공격에 사용된 Techniques은 아래 [표 3]으로 식별된다.

[표 3] Konni Mitre Attack 침해 지표

Tatic	Technique	Description
Reconnaissance	T1598.002	Phishing for Information: Spearphishing Attachment
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1059.005	Command and Scripting Interpreter: Visual Basic
	T1204.002	User Execution: Malicious File
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Defense Evasion	T1027.001	Obfuscated Files or Information: Binary Padding
	T1027.010	Obfuscated Files or Information: Command Obfuscation
	T1036.007	Masquerading: Double File Extension
	T1140	Deobfuscate/Decode Files or Information
Discovery	T1016	System Network Configuration Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1518	Software Discovery
Collection	T1005	Data from Local System
Command and Control	T1001	Data Obfuscation
	T1132.001	Data Encoding: Standard Encoding
Exfiltration	T1041	Exfiltration Over C2 Channel

5. 두 공격사례 비교 분석

Konni 공격 사례와 비교하기 위해, 2023년 4월에 발생한 APT37 그룹의 공격 사례를 분석하였다. APT37 그룹은 Reaper, Ricochet Chollima, ScarCruft 등으로도 알려져 있으며, 북한과 연계된 해킹 그룹으로 알려져 있다. 이 그룹은 적어도 2012년부터 활동을 이어오고 있으며, 주로 한국의 공공 및 민간 부문 조직들을 공격 대상으로 삼았다[2].

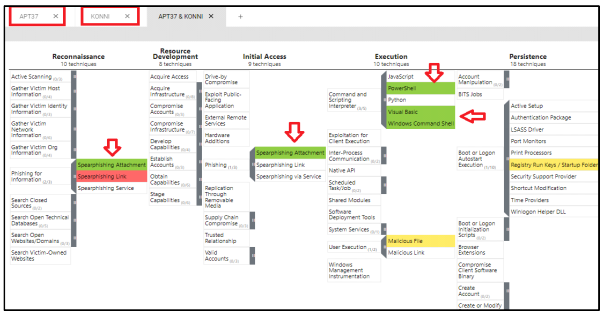
특히, APT37 그룹은 최근 4월부터 5월까지 과거 Konni 공격사례와 유사하게 대북 분야 기업을 타겟으로 삼아 이메일을 통한 스피어피싱 공격을 수행하였으며, 악성 파일로는 MS Word DOC 문서 파일과 LNK 바로가기 파일 형식을 이용하였다[3].

5.1 Mitre ATTACK 침해 지표 비교

APT37과 Konni 두 공격사례의 공격 유사성을 분석하기 위해, Mitre ATTACK에서 제공하는 Matrix 기능을 활용하였다. [그림 9]에서 붉은색으로 표시된 공격 기술은 APT37 그룹이 사용한 기술을 나타내고, 노란색으로 표시된 공격 기술은 Konni 악성코드에서 사용된 기술이다. 초록색으로 표시된 공격 기술은 두 공격사례에서 중복적으로 사용된 기술을 나타낸다.

두 공격사례는 Reconnaissance(자원 탐색), Initial Access(초기접근), Execution(실행), Defense Evasion (탐지 회피), Credential Access(인증 정보 획득) 전술 단계에서 중복된 기술들을 확인하였으며, [표 4]는 두 공격사례에서 중복된 Mitre Technique 정보를 표 형식으로 제시하였다.

이처럼, 보안 관련 기업이나 국가기관에서 침해 사례가 발생한 경우, 분석을 통해 공격그룹을 식별하고, 과거의 침해 사례들과 비교하여 유사점을 발견할 때, Mitre ATTACK 침해 지표를 활용함으로써 더 큰 신뢰성을 부여할 수 있다.



[그림 9] 두 공격사례 Mitre ATTACK Matrix 시각화 비교

[표 4] APT37, Konni 두 공격사례 간 중복된 Mitre Attack Techniques

Tatic	Technique	Description
Reconnaissance	T1598.002	Phishing for Information: Spearphishing Attachment
Resource Development	T1566.001	Phishing: Spearphishing Attachment
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1059.005	Command and Scripting Interpreter: Visual Basic
	T1204.002	User Execution: Malicious File
Defense Evasion	T1027.010	Obfuscated Files or Information: Command Obfuscation
Crendential Acces	T1083	File and Directory Discovery
	T1082	System Information Discovery

6. 결론

악성코드 분석을 수행하면서, 정적 분석과 동적 분석을 통해 식별되는 공격 기법, IP, C2 서버, 도메인 정보 등을 활용하여 특정 공격자 및 공격그룹을 식별하고 유사성을 식별할 수 있었다. Mitre ATTACK framework를 활용하여 과거 발생한 사례들 사이에서 초기접근부터 영향 단계까지 사용된 공격 기술을 비교함으로써, 공격 흐름의 유사성 또는 동일성을 식별하고, 이를 통해 공격자를 특정하기 위한 논리적인 근거를 제시하였다.

보안 관련 기업과 국가기관은 향후 침해 사건 분석과 공격그룹 특정을 위해 공격 사례의 특정 시그니처 데이터와 Mitre 침해 지표 데이터를 임의의 형식으로 가공해야 한다. 가공된 데이터는 저장되며, 향후 일정 기간 동안 발생하는 침해 사건을 분석하고 공격그룹 특정에 유용한 정보를 제공할 것으로 기대된다. 이를 통해, 보안 대비를 강화하고 기대 효과를 얻을 것으로 예상된다.

참고문헌

[1] 한국인터넷진흥원, “2023년 상반기 사이버 위협 동향 보고서”, pp. 4-6, 08월, 2023년.

[2] SOC PRIME, “APT37 Detection: North Korean Hackers Distribute Konni RAT, Target Orgs in Czechia and Poland”, 07월, 2023년.

[3] 지니어스, “북한인권단체를 사칭한 APT37 공격 사례”, pp. 2, 05월, 2023년.