MITRE ATT&CK 을 활용한 플랫폼과 분석

We know information security Better – NPcore

CONTENT
REVIEW

01

MITRE ATT&CK ?

개념과 정의

MITRE | ATT&CK®

사이버 공격자들의 최신 공격 기술 정보가 저장된 저장소

- 미국 국가안보관련 업무 수행 비영리 연구개발 단체 MITRE (마이터)
- 실제 사이버 공격 사례를 바탕으로 킬체인 단계를 자체적으로 개발하여 정리
- 사이버 공격 행위에 대해 14개의 공격기법과 (Tactics)과 218개의 기술(Technique) 관점으로 분석 정리

개념과 정의

MITRE | ATT&CK®

해커 그룹

사용 기법

악성 코드

공격 기법

MITRE ATT&CK
구성 – 1

해커가 사용하는 사이버 공격 및 악성코드 기법에 대해 14개의 전술과 218개의 기법으로 분류

파일 또는 정보 난독화/디코드

공격자는 난독화된 파일 또는 정보 를 사용 하여 분석에서 침입의 인공물을 숨길 수 있습니다. 정보를 사용하려는 방식에 따라 해당 정보를 디코딩하거나 난독화하기 위해 별도의 메커니즘이 필요할 수 있습니다. 이를 수행하는 방법에는 맬웨어의 기본 제공 기능이나 시스템에 있는 유틸리티를 사용하는 방법이 있습니다.

그러한 예 중 하나는 certutil 을 사용 하여 인증서 파일 안에 숨겨진 원격 액세스 도구 휴대용 실행 파일을 디코딩하는 것입니다. [1] 또 다른 예는 Windows `copy /b` 명령을 사용하여 바이너리 조각을 악성 페이로드로 재조립하는 것입니다. [2]

때때로 사용자 실행 의 일부로 난독화 또는 암호 해독을 위해 이를 여는 데 사용자의 작업이 필요할 수 있습니다 . 사용자는 공격자가 제공한 암호로 보호된 압축/암호화 파일을 열기 위해 암호를 입력해야 할 수도 있습니다. [삼]

아이디: T1140
하위 기술: 하위 기술 없음
ⓘ 전술: 방어 회피
ⓘ 플랫폼: Linux, Windows, macOS
ⓘ 필요한 권한: 사용자
ⓘ 방어 우회: 안티바이러스, 호스트 침입 방지 시스템, 네트워크 침입 탐지 시스템, 서명 기반 탐지
기고자: Matthew Demaske, Adaptforward; 레드 카나리

구성 – 2

TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005
정찰	자원개발	초기 액세스	실행	지속유지	권한획득	방어회피
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion

TA0040	TA0010	TA0011	TA0009	TA0008	TA0007	TA0006
타격	유출	명령제어	수집	측면이동	타겟발견	자격증명
Impact	Exfiltration	Command and Control	Collection	Lateral Movement	Discovery	Credential Access

218개의 Techniques

T1566

피싱

하위 기술 (3)

공격자는 피해자 시스템에 액세스하기 위해 피싱 메시지를 보낼 수 있습니다. 모든 형태의 피싱은 전자적으로 전달되는 사회 공학입니다. 스피어피싱으로 알려진 피싱은 표적이 될 수 있습니다. 스피어피싱에서는 특정 개인, 회사 또는 산업이 공격자의 표적이 됩니다. 보다 일반적으로 공격자는 대규모 악성코드 스팸 캠페인과 같이 표적이 아닌 피싱을 수행할 수 있습니다.

공격자는 일반적으로 피해자 시스템에서 악성 코드를 실행하기 위해 악성 첨부 파일이나 링크가 포함된 이메일을 피해자에게 보낼 수 있습니다. 피싱은 소셜 미디어 플랫폼과 같은 제3자 서비스를 통해서도 수행될 수 있습니다. 피싱에는 신뢰할 수 있는 출처로 가장하는 것과 같은 사회 공학 기술이 포함될 수도 있습니다.

아이디: T1566
하위 기술: T1566.001 , T1566.002 , T1566.003
전술: 초기 접근
플랫폼: Google Workspace, Linux, Office 365, SaaS, Windows, macOS
데이터 소스: 애플리케이션 로그 : 애플리케이션 로그 콘텐츠, 네트워크 트래픽 : 네트워크 트래픽 콘텐츠, 네트워크 트래픽 : 네트워크 트래픽 흐름
CAPEC ID: CAPEC-98
기여자: 필립 윈더
버전: 2.1
작성일: 2020년 3월 2일
최종 수정일: 2021년 4월 14일

T1113

화면 캡처

공격자는 작업 과정에서 정보를 수집하기 위해 데스크톱의 화면 캡처를 시도할 수 있습니다. 화면 캡처 기능은 침해 후 작업에 사용되는 원격 액세스 도구의 기능으로 포함될 수 있습니다. 스크린 샷을 가지고가는 것은 원시 유틸리티 또는 API 호출 등을 통해 일반적 가능하다 `CopyFromScreen`, `xwd` 또는 `screencapture`. [1] [2]

아이디: T1113
하위 기술: 하위 기술 없음
전술: 수집
플랫폼: Linux, Windows, macOS
데이터 출처 : Command : Command 실행, Process : OS API 실행
CAPEC ID: CAPEC-648
버전: 1.1
작성일: 2017년 5월 31일
최종 수정일: 2020년 3월 24일

구성 – 4

APT19	Codoso, C0d0so0, Codoso 팀, Sunshop Group	APT19 는 방위, 금융, 에너지, 제약, 통신, 하이테크, 교육, 제조 및 법률 서비스를 포함한 다양한 산업을 표적으로 삼는 중국 기반 위협 그룹입니다. 2017년에는 7개의 법률 및 투자 회사를 대상으로 피싱 캠페인이 사용되었습니다. 일부 분석가는 APT19 와 Deep Panda 를 같은 그룹으로 추적하지만 그룹이 동일한지 오픈 소스 정보에서 명확하지 않습니다.
APT28	SNAKEMACKEREL, Swallowtail, 그룹 74, Sednit, Sofacy, Pawn Storm, 팬시 베어, STRONTIUM, Tsar 팀, 위협 그룹-4127, TG-4127	APT28 은 러시아의 GRU(General Staff Main Intelligence Directorate) 85 GTsSS(Main Special Service Center) 군부대 26165로 추정되는 위협 그룹입니다. 이 그룹은 최소 2004년부터 활동해 왔습니다. APT28 은 2016년 힐러리 클린턴 캠페인, 민주당 전국위원회, 민주당 하원 선거운동위원회를 해킹해 미 국

해커 그룹

사용 기법

사용된 기술

ATT&CK® 네비게이터 레이어

도메인	ID		이름	사용
기업	T1134	.001	액세스 토큰 조작 : 토큰 사칭/도용	APT28 은 CVE-2015-1701을 사용하여 SYSTEM 토큰에 액세스하고 권한 상승의 일부로 이를 현재 프로세스에 복사했습니다. [23]
기업	T1098	.002	계정 조작 : 이메일 대리인 권한 교환	APT28 은 Powershell cmdlet을 사용 `ApplicationImpersonation` 하여 손상된 계정에 역할을 부여했습니다. [2]
기업	T1583	.001	인프라 획득 : 도메인	NATO, OSCE 보안 웹사이트, 코카서스 정보 자원 및 기타 조직을 모방한 APT28 등록 도메인. [6] [14]
기업	T1595	.002	액티브 스캐닝 : 취약점 스캐닝	APT28 은 취약한 서버를 찾기 위해 대규모 스캔을 수행했습니다. [24]
기업	T1071	.001	응용 계층 프로토콜 : 웹 프로토콜	CHOPSTICK 와 같이 APT28 에서 사용하는 이후의 임플란트 는 모듈 구성에 따라 C2에 대해 HTTP, HTTPS 및 기타 합법적인 채널을 혼합하여 사용합니다. [6] [2]
		.003	응용 계층 프로토콜 : 메일 프로토콜	APT28 은 자체 등록된 Google 메일 계정을 사용하고 나중에 피해자의 이메일 서버를 손상시키는 것을 포함하여 다양한 임플란트의 통신 채널에 IMAP, POP3 및 SMTP를 사용했습니다. [6] [2]

구성 – 5

S0575	콘티		Conti 는 2019년 12월에 처음 관찰된 Ransomware-as-a-Service이며 TrickBot 을 통해 배포되고 있습니다. 그것은 주요 기업과 정부 기관, 특히 북미 지역에 사용되었습니다. 다른 랜섬웨어 제품군과 마찬가지로 Conti 를 사용하는 행위자 는 손상된 네트워크에서 민감한 파일과 정보를 훔치고 몸값을 지불하지 않으면 이 데이터를 게시하겠다고 위협합니다.
S0492	쿠키마이너		CookieMiner 는 암호화폐 거래소와 관련된 정보를 노리고 피해자 시스템 자체에서 암호화폐 채굴을 가능하게 하는 맥 기반 악성코드입니다. 2019년 야생에서 처
S0212	코랄덱		
S0137	코어 쉘	소파, SOURFACE	

악성 코드

공격 기법

사용된 기술

ATT&CK® 네비게이터 레이어

도메인	ID		이름	사용
기업	T1059	.003	명령 및 스크립팅 인터프리터 : Windows 명령 셸	Conti 는 명령줄 옵션을 활용하여 공격자가 파일을 스캔하고 암호화하는 방법을 제어할 수 있습니다. [2]
기업	T1486		영향을 위해 암호화된 데이터	Conti 는 `CreateIoCompletionPort()`, `PostQueuedCompletionStatus()` 및 `GetQueuedCompletionPort()` 를 사용하여 .exe, .dll 및 .lnk 확장자를 가진 파일을 제외하고 파일을 빠르게 암호화할 수 있습니다. 각 피해자에 대해 고유한 번들 RAS-4096 공개 암호화 키와 함께 파일마다 다른 AES-256 암호화 키를 사용했습니다. Conti 는 "Windows 다시 시작 관리자"를 사용하여 파일이 잠금 해제되고 암호화를 위해 열 수 있는지 확인할 수 있습니다. [1] [2] [3] [4]
기업	T1140		파일 또는 정보 난독화/디코드	Conti 는 하드코딩된 AES-256 키를 사용하여 페이로드를 해독했습니다. [1] [2]
기업	T1083		파일 및 디렉토리 검색	Conti 는 로컬 시스템에서 파일을 검색할 수 있습니다. [2]
기업	T1490		시스템 복구 금지	Conti 는 를 사용하여 Windows 볼륨 섀도 복사본을 삭제할 수 있습니다 `vssadmin`. [2]
기업	T1106		네이티브 API	Conti 는 실행 중에 API 호출을 사용했습니다. [1] [2]

02

MITRE ATT&CK 기대 및 효과 (솔루션)

활용 이전

Analysis start

솔루션이 보유한 패턴에 의해 단순 구분

Nomal or Malware

과정은 오로지 패턴 유무 뿐 !!

“이 파일이 무엇을 하였나요?”

MITRE ATT&CK
활용 이후

이름	설명	심각성	ATT&CK 테크닉	기술 ID
antidbg_devices	디버거 및 포렌식 도구에서 알려진 장치가 있는지 확인합니다.	높은	프로세스 검색 , 파일 및 디렉터리 검색	T1057 , T1083
antidbg_windows	디버거 및 포렌식 도구에서 알려진 창의 존재 여부 확인	높은	프로세스 디스커버리	T1057
antivm_generic_bios	Anti-virtualization을 위해 Bios 버전을 확인합니다.	높은		
지속성_자동 실행	Windows 시작 시 자동 실행을 위해 자체 설치	높은	예약된 작업 , 레지스트리 실행 키/시작 폴더	T1053 , T1060
우회_방화벽	로컬 방화벽의 정책 및 설정에 따라 작동	높은	기존 서비스 수정	T1031
수정_인증서	시스템 인증서 생성 또는 수정 시도	높은	레지스트리 수정	T1112
ransomware_message	잠재적인 몸값 메시지를 디스크에 씁니다.	높은		
antivm_vbox_keys	레지스트리 키의 존재를 통해 VirtualBox 감지	높은	쿼리 레지스트리 , 프로세스 검색	T1012 , T1057
antivm_vmware_in_instruction	명령어 기능을 통해 VMWare 감지	높은		
안티에뮤_와인	Wine 에뮬레이터의 존재 감지	높은	프로세스 디스커버리	T1057
할당_rwx	읽기-쓰기-실행 메모리 할당(일반적으로 자체 압축 풀기)	중간		
antisandbox_sleep	프로세스에서 분석 작업을 지연시키려고 했습니다.	중간		
create_exe	파일 시스템에 실행 파일 생성	중간	모듈 로드를 통한 실행	T1129
서비스 생성	서비스 생성	중간	새 서비스 설치 , 기존 서비스 수정	550 , T1031
스텔스_창	프로세스가 숨겨진 창을 생성했습니다.	중간	숨겨진 창	T1143
주입_프로세스_검색	잠재적으로 실행 중인 프로세스를 검색하여 샌드박스 회피, 코드 주입 또는 메모리 덤프에 대한 프로세스를 식별합니다.	중간	프로세스 디스커버리	T1057

이상행위에 대한 표준화

기대 및 효과 – 1

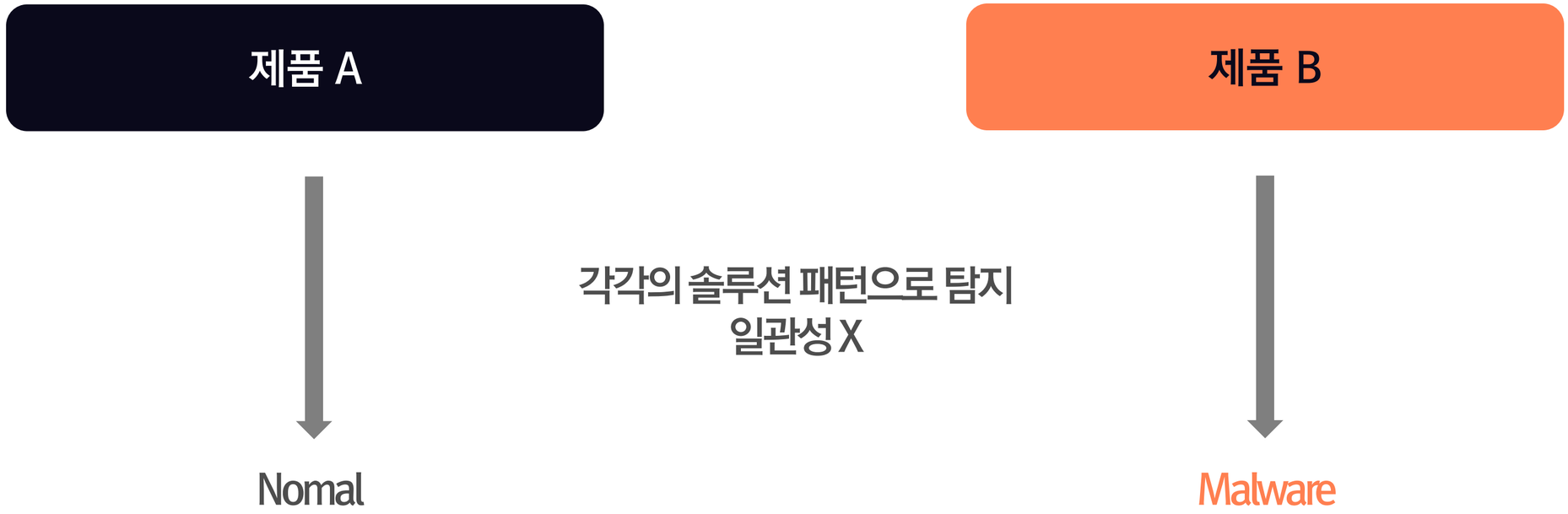
01 사이버 공격 행위에 대한 “공통된 언어”로 사용되도록 역할

02 공격 방식이나 취약점, 공격자들의 패턴을 누구나 이해할 수 있게 설명

03 프레임을 사용할 수록 보안 커뮤니티 전체가 빠르고 이해하기 쉬움

기대 및 효과 – 2

동일 파일/행위에 대한 탐지 해석이 달라 혼란



“그래서 뭐가 맞는 건데요?”

기대 및 효과 – 3

행위 분석에 대한 표준화된 공통 Rule 정립

– 솔루션에 의한 유입 파일 분석 프로세스 –

03

MITRE ATT&CK 활용 및 연동 플랫폼

활용 및 연동분야

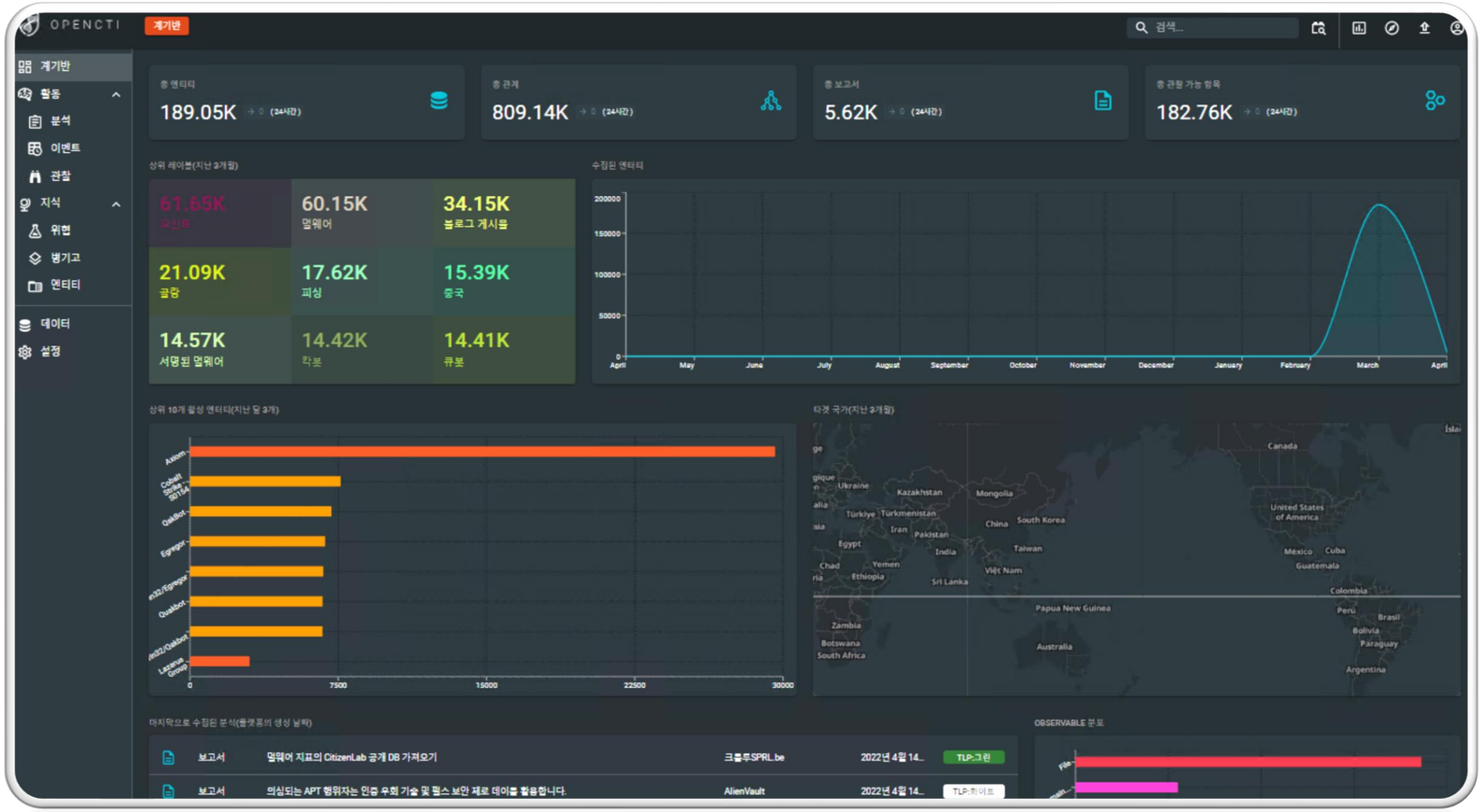
MITRE | ATT&CK®

- 위협정보 공유플랫폼 연동
- 사이버 공격 사례 보고서 분석
- 정적분석 활용
- 동적분석 플랫폼 활용
- 보안솔루션

활용 – 위협정보 공유 플랫폼 연동

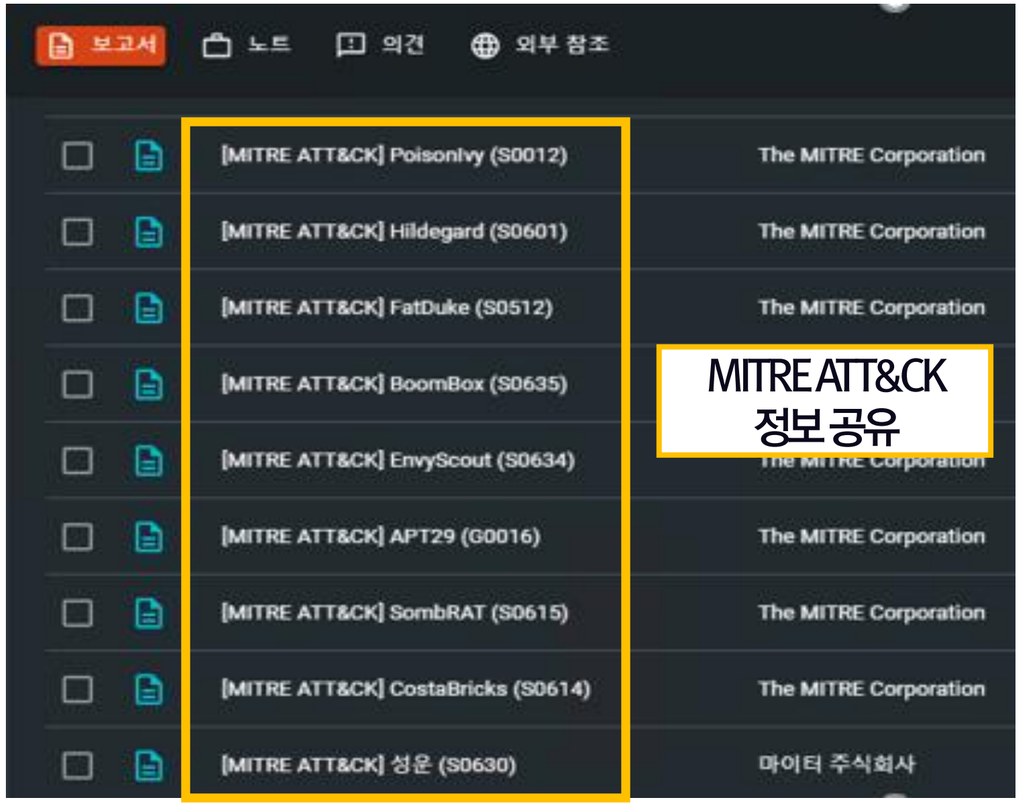
OPENCTI

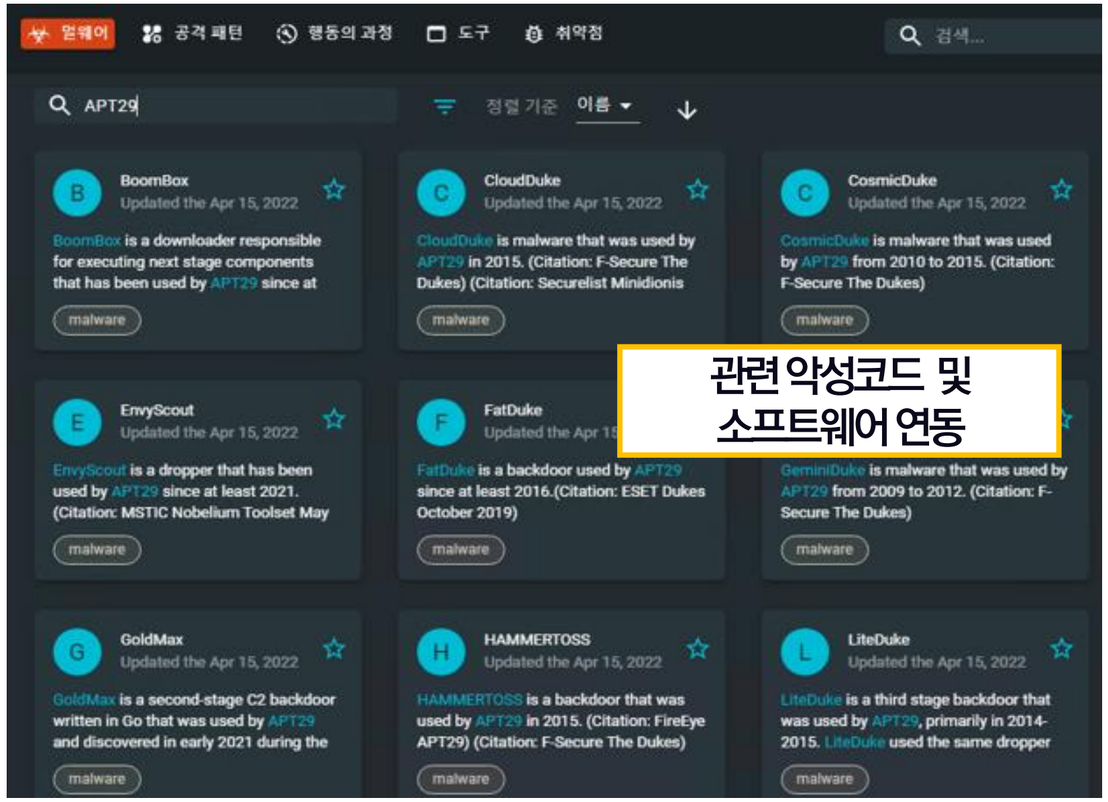
오픈소스 기반
사이버위협정보
공유플랫폼



활용 – 위협정보 공유 플랫폼 연동

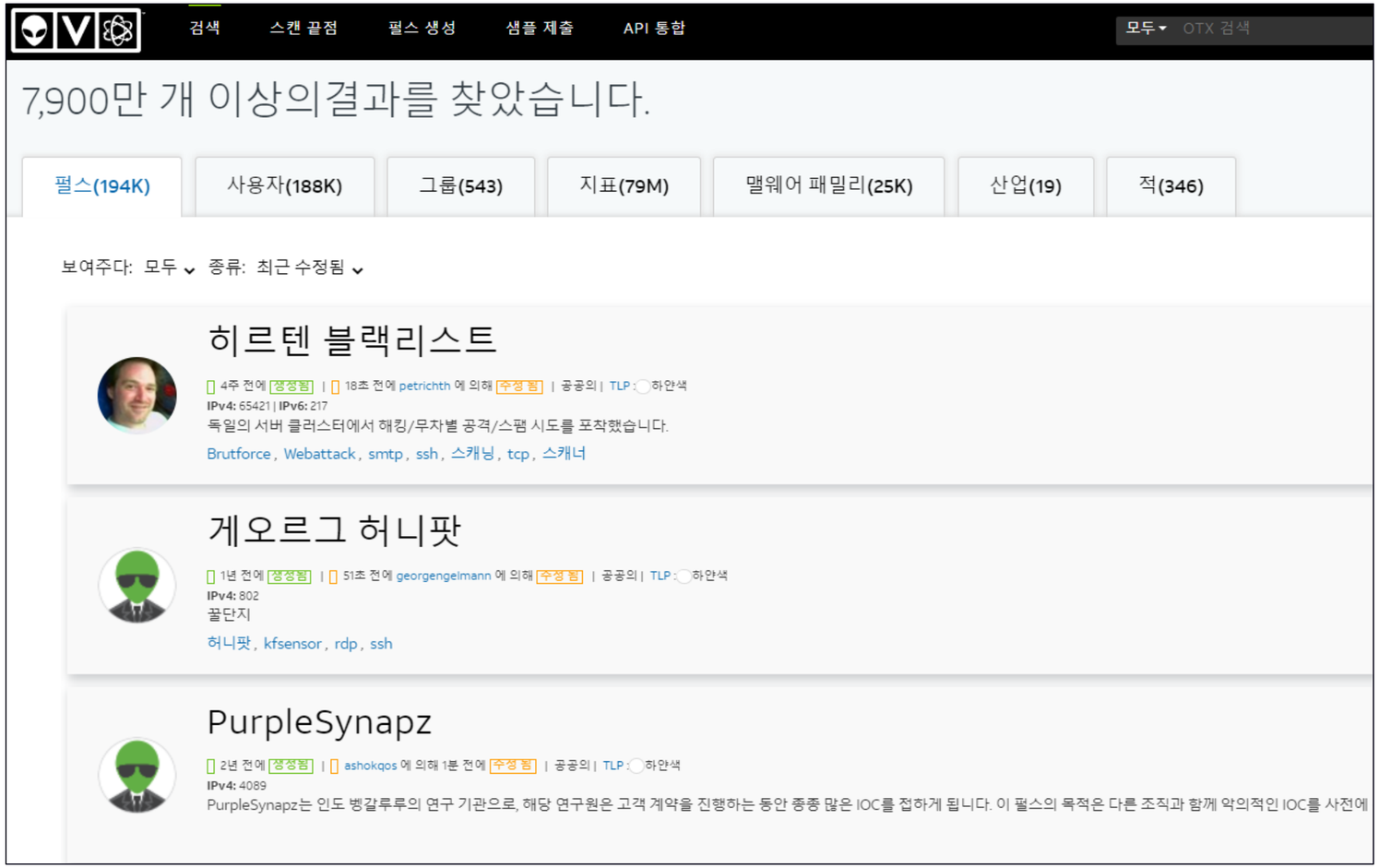
MITRE ATT&CK 에서 제공하는 사이버 공격 그룹 정보 및 관련 악성코드 연동





활용 – 위협정보 공유 플랫폼 연동

개방형
위협 인텔리전스
커뮤니티



MITRE ATT&CK

활용 – 위협정보 공유 플랫폼 연동

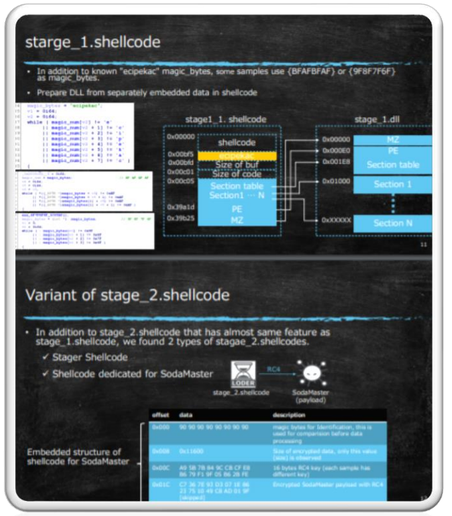
이름	설명	심각성	ATT&CK 테크닉	기술 ID
antidbg_devices	디버거 및 포렌식 도구에서 알려진 장치가 있는지 확인합니다.	높은	프로세스 검색 , 파일 및 디렉터리 검색	T1057 , T1083
antidbg_windows	디버거 및 포렌식 도구에서 알려진 창의 존재 여부 확인	높은	프로세스 디스커버리	T1057
antivm_generic_bios	Anti-virtualization을 위해 Bios 버전을 확인합니다.	높은		
지속성_자동 실행	Windows 시작 시 자동 실행을 위해 자체 설치	높은	예약된 작업 , 레지스트리 실행 키/시작 폴더	T1053 , T1060
우회_방화벽	로컬 방화벽의 정책 및 설정에 따라 작동	높은	기존 서비스 수정	T1031
수정_인증서	시스템 인증서 생성 또는 수정 시도	높은	레지스트리 수정	T1112
ransomware_message	잠재적인 몸값 메시지를 디스크에 씁니다.	높은		
antivm_vbox_keys	레지스트리 키의 존재를 통해 VirtualBox 감지	높은	쿼리 레지스트리 , 프로세스 검색	T1012 , T1057
antivm_vmware_in_instruction	명령어 기능을 통해 VMWare 감지	높은		
안티에뮤_와인	Wine 에뮬레이터의 존재 감지	높은	프로세스 디스커버리	T1057
할당_rwx	읽기-쓰기-실행 메모리 할당(일반적으로 자체 압축 풀기)	중간		
antisandbox_sleep	프로세스에서 분석 작업을 지연시키려고 했습니다.	중간		
create_exe	파일 시스템에 실행 파일 생성	중간	모듈 로드를 통한 실행	T1129
서비스 생성	서비스 생성	중간	새 서비스 설치 , 기존 서비스 수정	550 , T1031
스텔스_창	프로세스가 숨겨진 창을 생성했습니다.	중간	숨겨진 창	T1143
주입_프로세스_검색	잠재적으로 실행 중인 프로세스를 검색하여 샌드박스 회피, 코드 주입 또는 메모리 덤프에 대한 프로세스를 식별합니다.	중간	프로세스 디스커버리	T1057

활용 – 사이버 공격사례 보고서 분석

2021

- Oct 19 - [Proofpoint] Whatta TA: TA505 Ramps Up Activity, Delivers New FlawedGrace Variant |
- Oct 19 - [Trend Micro] PurpleFox Adds New Backdoor That Uses WebSockets |
- Oct 18 - [Symantec] Harvester: Nation-state-backed group uses new toolset to target victims in South Asia |
- Oct 12 - [Kaspersky] MysterySnail attacks with Windows zero-day |
- Oct 06 - [Cybereason] Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms |
- Oct 04 - [JP-CERT] Malware Gh0stTimes Used by BlackTech |
- Sep 30 - [Kaspersky] GhostEmperor: From ProxyLogon to kernel mode |
- Sep 27 - [Microsoft] FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor |
- Sep 23 - [ESET] FamousSparrow: A suspicious hotel guest |
- Sep 14 - [McAfee] Operation 'Harvest': A Deep Dive into a Long-term Campaign |
- Sep 13 - [Trend Micro] APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs |
- Sep 09 - [Recorded Future] Dark Covenant: Connections Between the Russian State and Criminal Actors |
- Sep 08 - [Fireeye] Pro-PRC Influence Campaign Expands to Dozens of Social Media Platforms, Websites, and Forums in at Least Seven Languages, Attempted to Physically Mobilize Protesters in the U.S. |
- Aug 25 - [Bitdefender] FIN8 Threat Actor Spotted Once Again with New "Sardonic" Backdoor |

2006 ~ 2022년 까지 전세계의 약1,300 여개의
사이버 공격 사례 등록

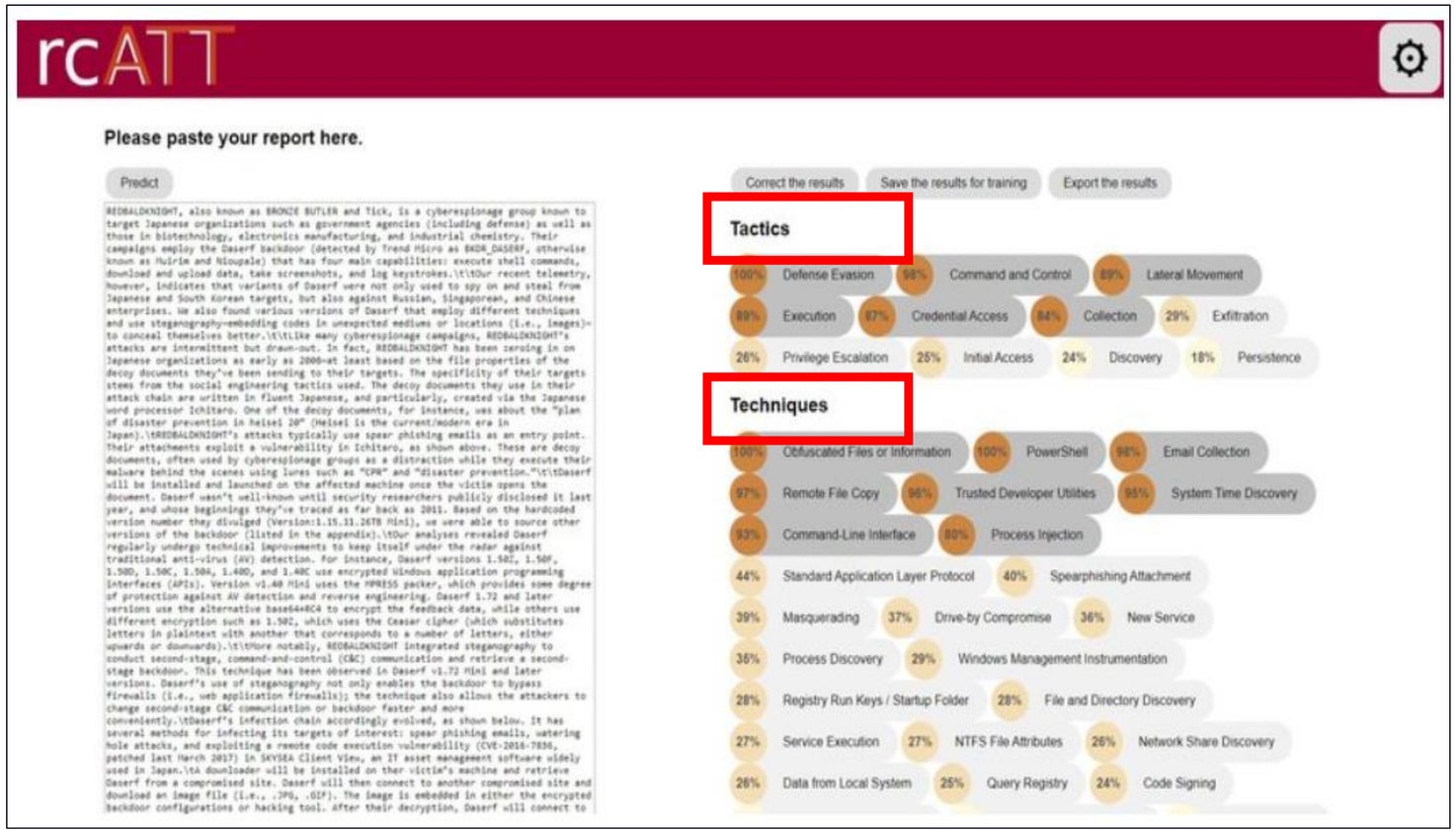


크고 작은 사이버 공격 이슈에 대한 분석

활용 – 사이버 공격사례 보고서 분석

rcATT

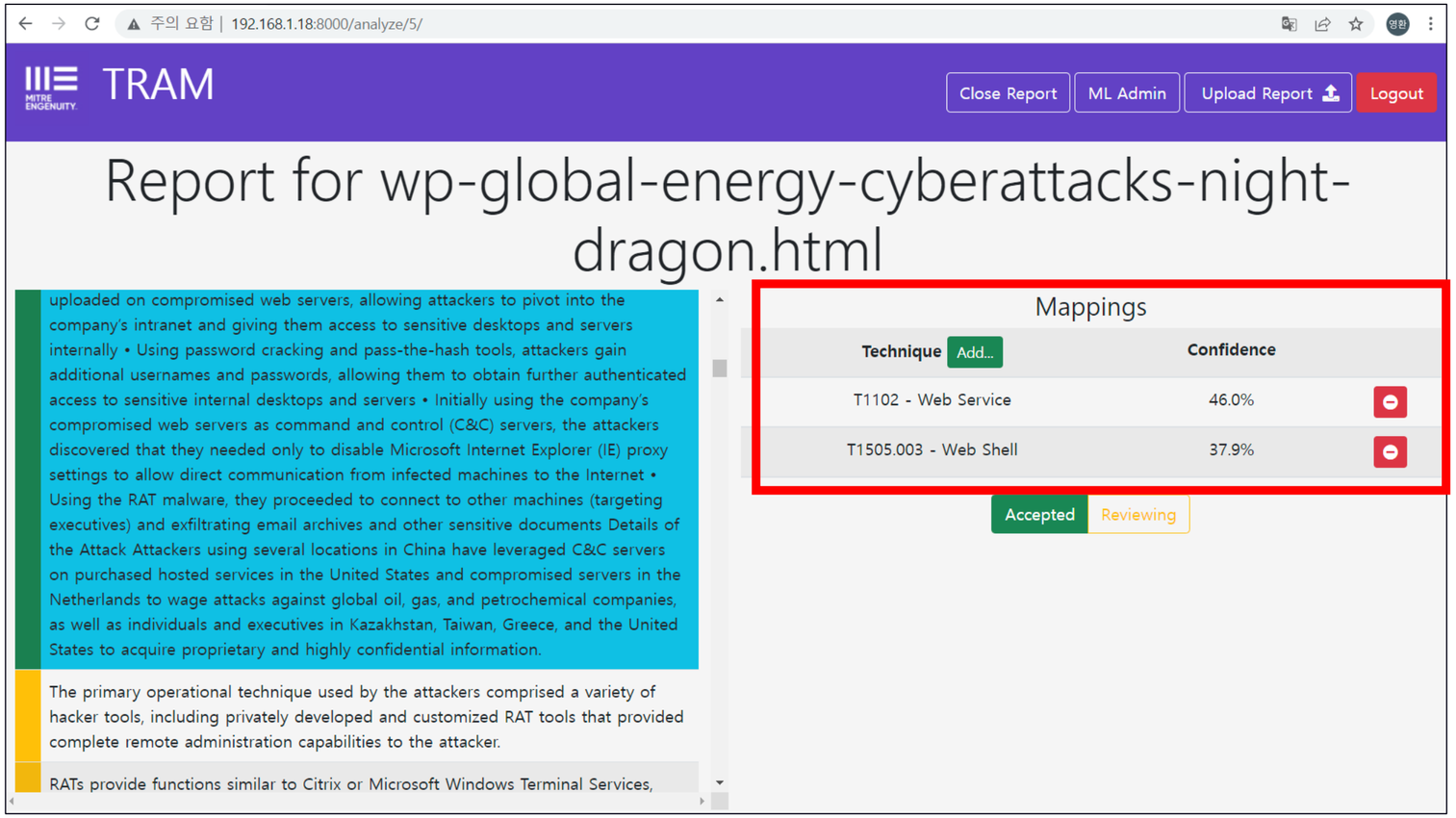
사이버 위협 보고서에 대해
MITRE ATT&CK 을 자동 태깅



활용 – 사이버 공격사례 보고서 분석

TRAM

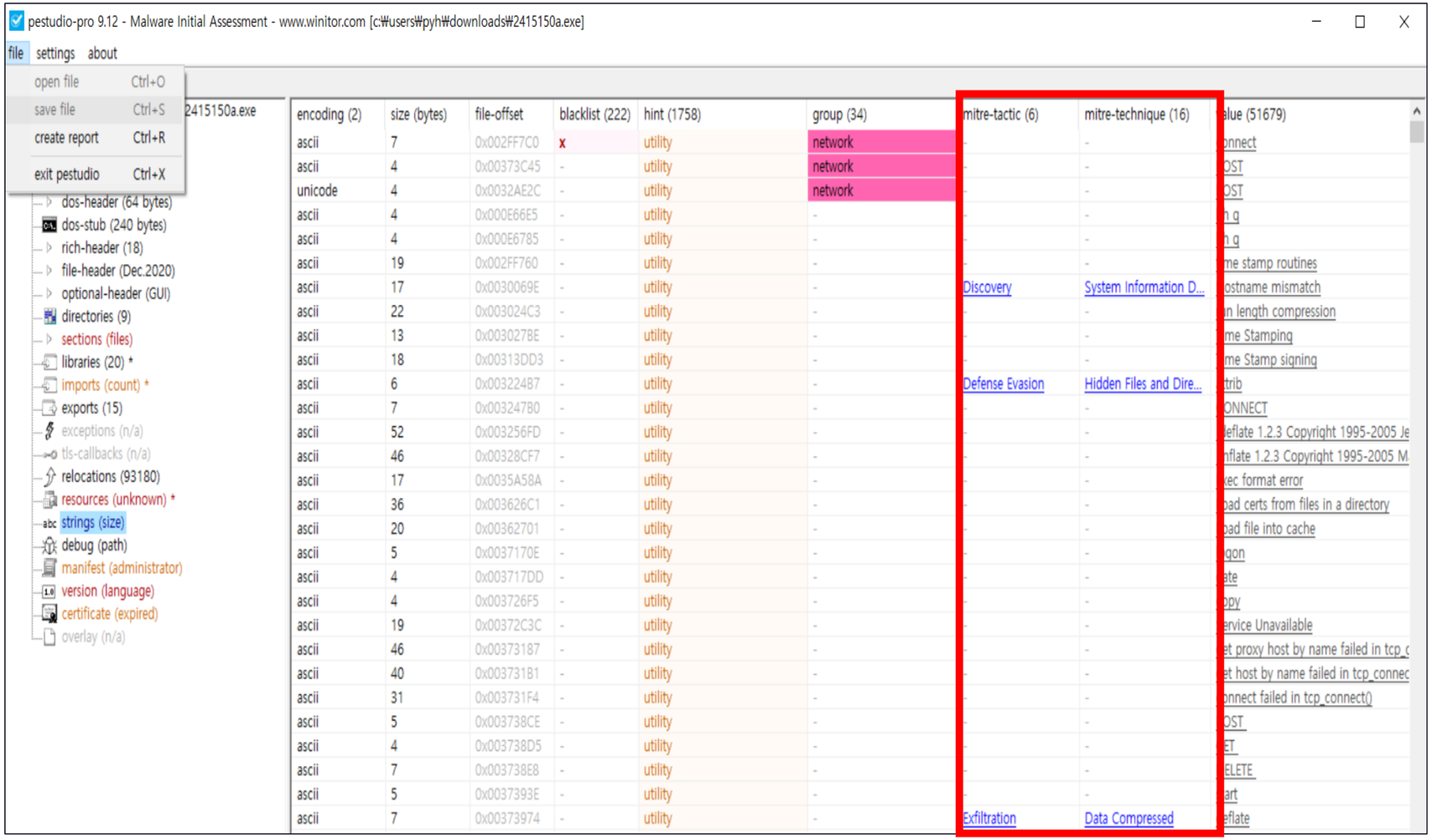
Threat Report
ATT&CK Mapper



활용 – 정적분석

PEStudio

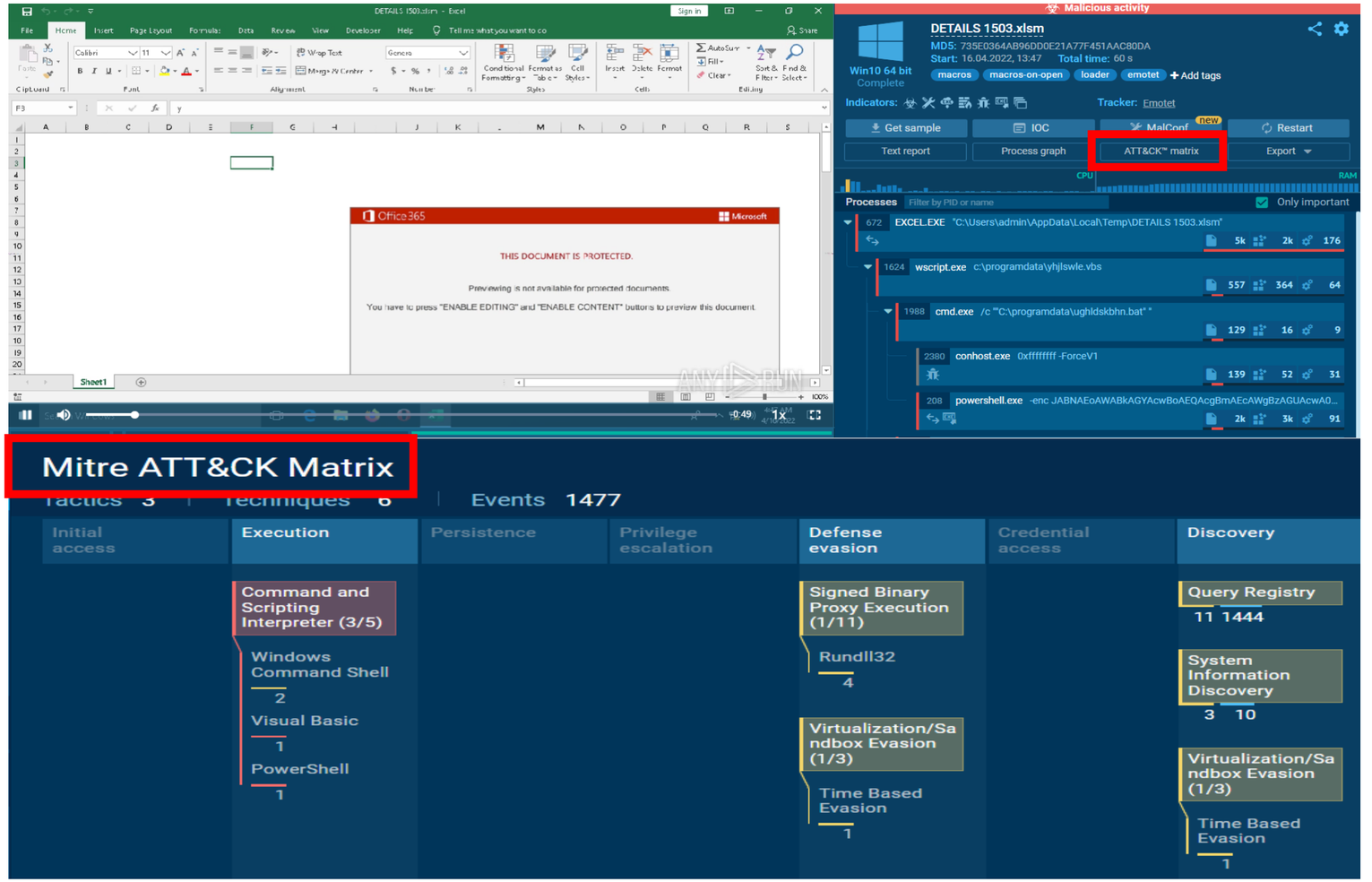
PE 파일 정적분석 툴



활용 – 동적분석 플랫폼

ANY RUN
INTERACTIVE MALWARE ANALYSIS

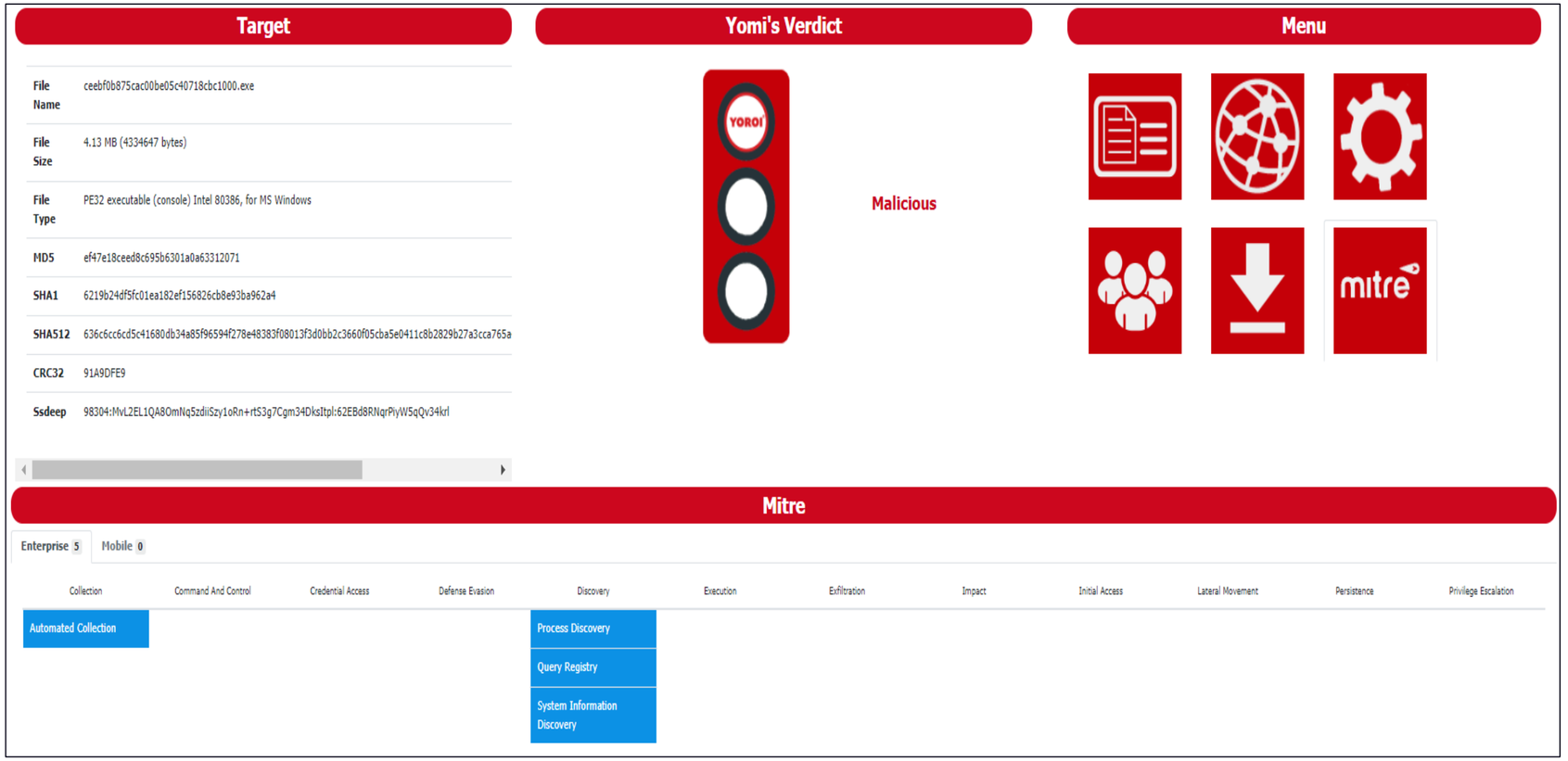
Sandbox 기반
동적분석 서비스
플랫폼



활용 – 동적분석 플랫폼

YOMI BY YOROI

Sandbox 기반
동적분석 서비스
플랫폼



활용 – 보안솔루션 (APT / EDR)

NPCORE

위험도

정적 아라를 탐지내역

YARA	MITRE	설명
Keylogger	T1179 T1129	Hooking, Execution through Module Load
DetectWindowsHook	T1179 T1129	Hooking, Execution through Module Load
SocialEngineering	T1106 T1073 T1527	Execution through API, DLL Side-Loading, Application Access Token
ExecutableFile	T1204	User Execution

후킹

Windows 프로세스는 종종 [illegible] 한 작업을 수행합니다. Window[illegible]

후킹에는 이러한 함수에 대한 호출 리디렉션이 포함되며 다음을 통해 구현할 수 있습니다.

- 메시지, 키 입력 및 마우스 입력과 같은 이벤트에 대한 응답으로 지정된 코드를 가로채서 실행하는 **후크 프로시저** . [1] [2]
- 가져온 API 함수에 대한 포인터가 저장되는 프로세스의 IAT에 대한 수정을 사용하는 **가져오기 주소 테이블(IAT) 후킹** . [2] [3] [4]
- 코드 흐름을 리디렉션하기 위해 API 함수의 첫 번째 바이트를 덮어쓰는 **인라인 후킹** . [2] [5] [4]

정적분석 에서의 MITRE ATT&CK 활용

EDR 및 동적분석에서 MITRE ATT&CK 활용

04

앞으로 NGAV의 방향

앞으로의 NGAV의 방향

MITRE | ATT&CK®

+

머신러닝 학습 및 AI 인공지능과의 조합으로
악성코드 탐지에 대한 신뢰도 확보

앞으로의 NGAV의 방향

사이버 보안 이벤트 발생

↓

관련 및 연계 행위로
MITRE ATT&CK 표준 자동화

→

구분	세부내용
TA0001	초기 엑세스
TA1566.001	스피어피싱 첨부파일
TA1566.002	스피어피링 링크
T1189	웹사이트 방문 스크립트 자동 실행
T1185	브라우저의 보안 취약성을 이용
TA0002	악성코드 실행
T1218.005	서명된 바이너리 프록시 실행
TA0007	발견 (타겟)
T1083	파일 및 디렉터리 검색
TA0009	수집 (목표)
T1546.001	기본파일 연결 변경
T1056.001	입력 캡처
T1059.006	명령 및 스크립팅 인터프리터
TA0010	유출
T1560	수집된 데이터 보관
T1114.003	이메일 수집
T1573.001	암호화된 채널
T1074.001	준비된 데이터 : 로컬 데이터 준비

알려지지 않은
신/변종 악성코드에 대해서
고차원적으로 대응

앞으로의 NGAV의 방향

알려진 악성코드 대응

AV

패턴 위주의 백신

알려지지 않은 악성코드 대응

APT

AV + 정적분석 + 동적분석의 APT (다차원분석)

알려지지 않은 악성코드 대응 **고도화**

NG AV

APT + (머신러닝 MITRE ATT&CK)

경청해주셔서
감사합니다