SAMSUNG SDS

REAL 2019

Realize your vision
through Digital Transformation

2019 . 5 . 8 . Wed . The Shilla Seoul

AI를 활용한

악성코드 탐지

김휘강 교수

About me

김휘강 교수
고려대학교

약력

- 2017.10 ~ 현재 AI.Spera 창업자
- 2015.03 ~ 현재 고려대학교 정보보호대학원, 사이버국방학과 부교수
- 2010.03 ~ 2015.02 고려대학교 정보보호대학원, 사이버국방학과 조교수
- 2004.05 ~ 2010.02 엔씨소프트, 정보보안실 실장/Technical Director
- 1999.08 ~ 2004.05 에이쓰리시큐리티컨설팅 (현 에이쓰리시큐리티) 창업자
- 2000.03 ~ 2009.02 KAIST 산업 및 시스템공학과 박사
- 1998.03 ~ 2000.02 KAIST 산업공학과 석사
- 1994.03 ~ 1998.02 KAIST 산업경영학과 학사

주요 연구 실적

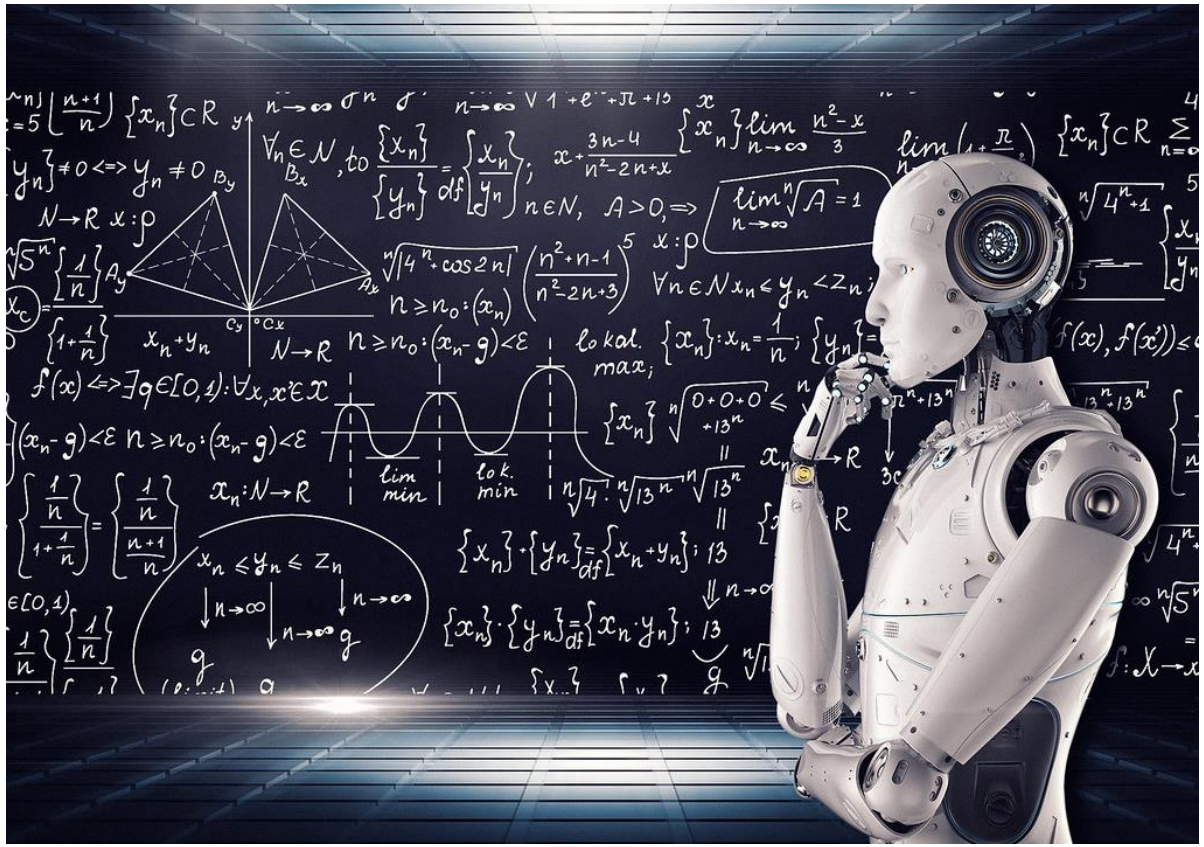
- International Conferences: **NDSS 2016, WWW (2014, 2017, 2018)**, MILCOM 2016, ACM NetGames (2013, 2014, 2015, 2017), IEEE VizSec (2017), OASIS Borderless Cyber and FIRST Tech. Symp. (2017)
- International Journals: IEEE Trans. On Information Forensics and Security (2017), Computer & Security (2016), Digital Investigation (2015)

Agenda

- AI/Machine Learning 시대의 보안
  - Intro
  - 국내외 동향
  - 정보보호 R&D 데이터챌린지 lesson learned
- 지능형 악성코드 탐지시스템 개발 사례
- Conclusion Remark

AI/MACHINE LEARNING 시대의 보안

Deep Learning(AlphaGo, AlphaGo-Zero)



Irreplaceable(a.대체불가능한) vs. Replaceable

어디까지 대체될 수 있을 것인가?

고부가가치 Job

- Irreplaceable!
- 생산성 여부와 관계없이 대체 불가능한 Job, 난이도가 높은 Job
  = Irreplaceable Job

**저부가가치,
노동집약적 Job**

- 기계(로봇), 자동화, 글로벌화에 의해 대체됨

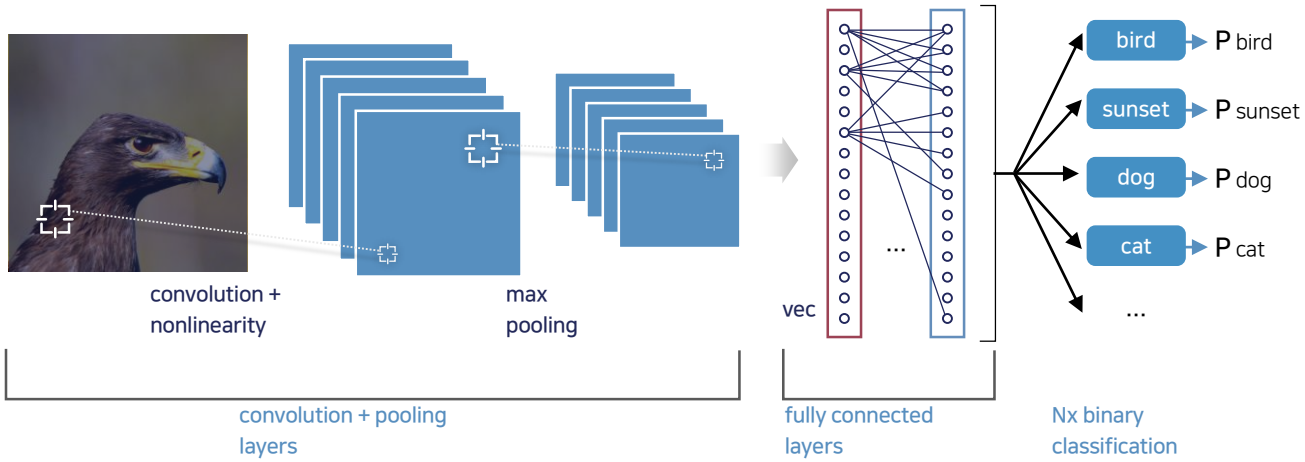
**보안업무는 기계에 의해
대체 불가능한가?**

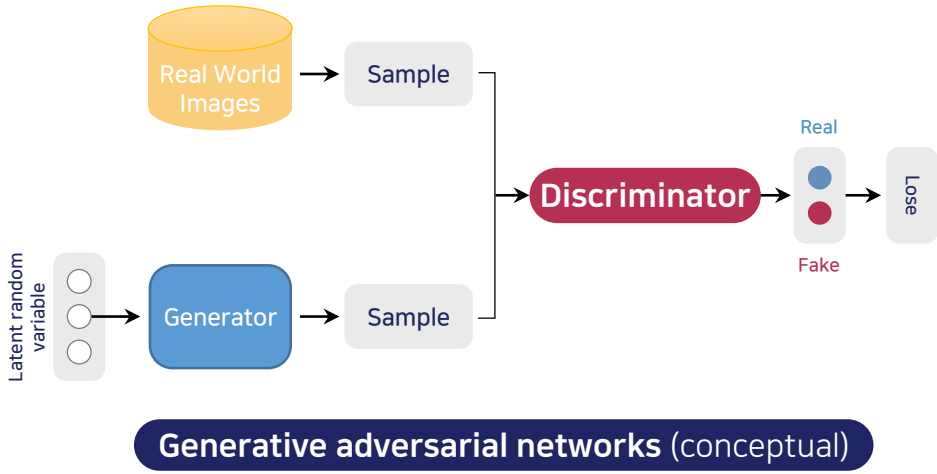
- Firewall, Log Analyzer, IDS, IPS, Port Scanner, Vulnerability Scanner, Web Scanner, Antivirus …
- 거의 모든 부분에서 전부 또는 일부 대체 가능

AI/ML (Machine Learning) + Security

What's New

- CNN(Convolutional Neural Network), DNN(Deep Neural Network)을 이용한 학습
- Streamline data
- Gan(Generative Adversarial Nets)을 이용한 Adversarial Data 생성





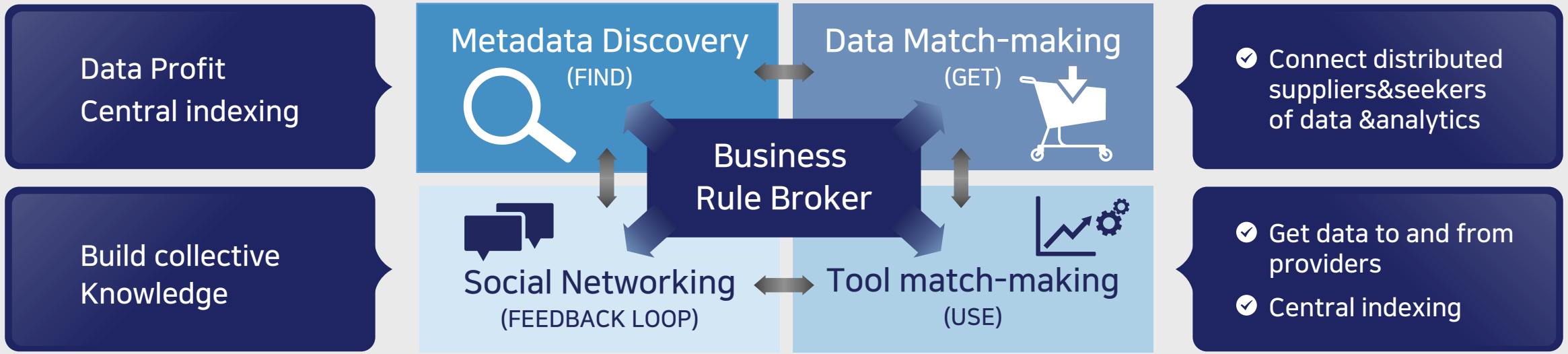
AI/ML (Machine Learning) + Security

What's still now New?

- 사람(적용에의 두려움)
- Data(양질의 data 부족)
- Blackbox algorithm + Adversarial Machine Learning attacks
- Reference
  - Image/Voice recognition에 훌륭한 CNN, DNN이 보안 분야에도 적용 잘 된다는 보장이 있는가?
- Scalability
  - IoT 시대에 경량화된 알고리즘이 중요해지는 시점에, local machine에서 learning을 할 수 있는 환경이 되는가?
- Privacy
  - 좋은 결과를 얻고는 싶지만, 내 민감 데이터를 주고 싶지는 않음

Automated Security/Data-Driven Security 동향 IMPACT

- IMPACT(The Information Marketplace for Policy and Analysis of Cyber-risk & Trust)
- 미 국토안보부(DHS) 지원으로 사이버 보안 연구에 필요한 데이터(1페타 이상) 공유
- 데이터 검색, 데이터&분석 도구 매칭, 데이터 공유, 소셜 서비스 제공

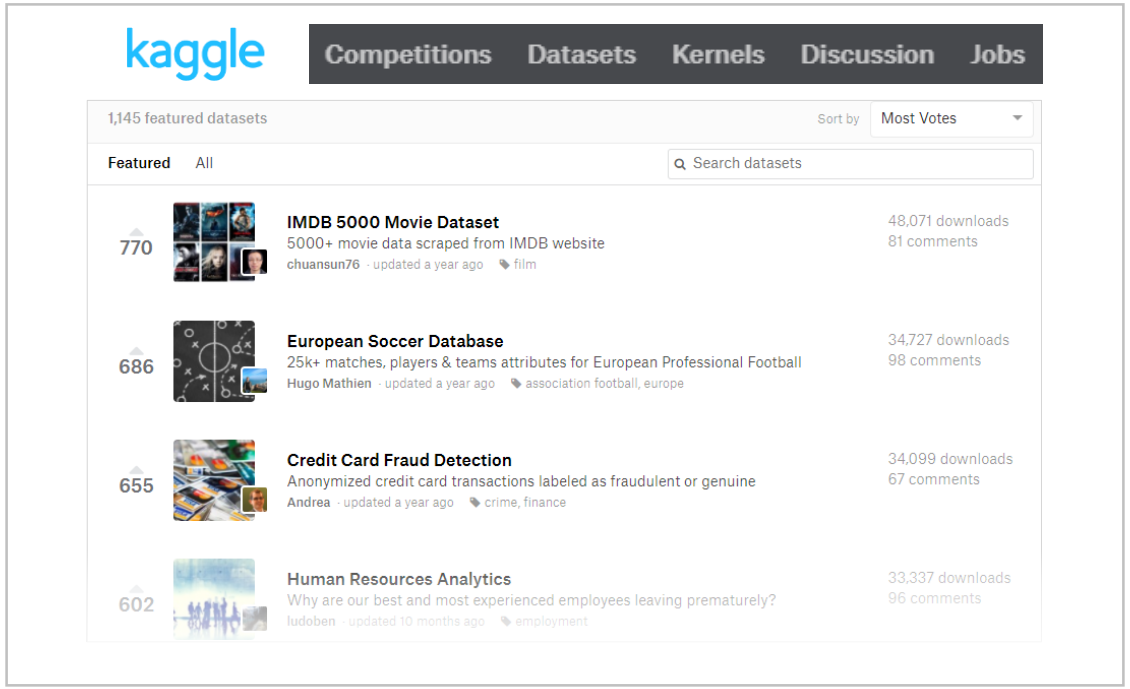


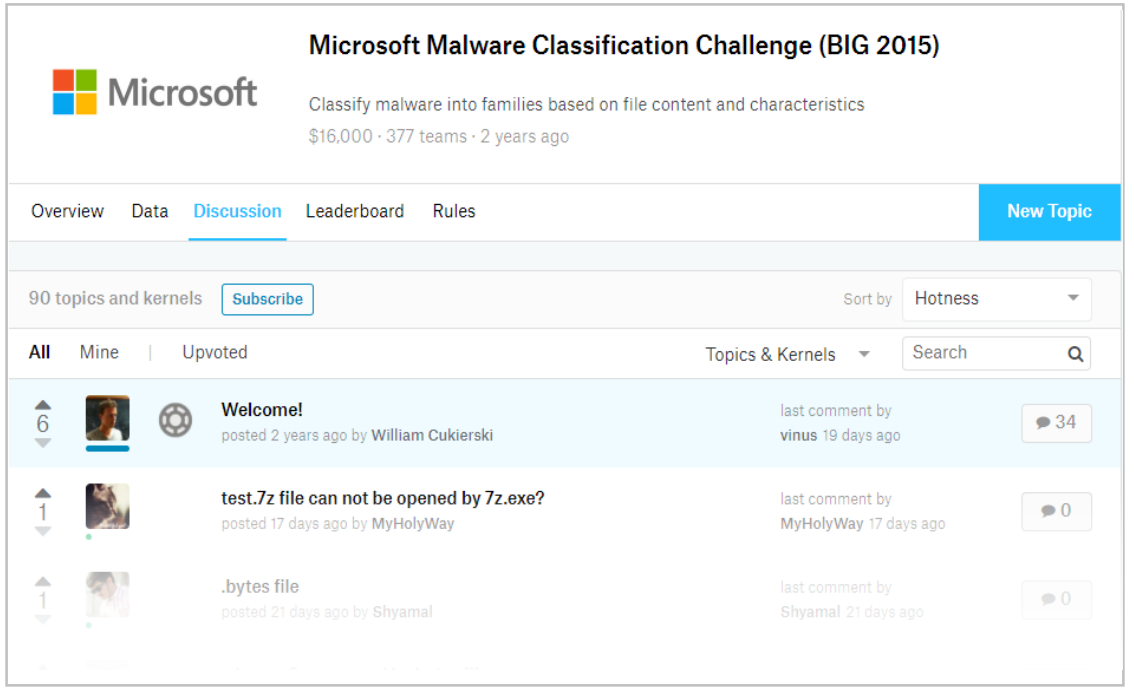
美 학계·산업계·비영리단체·정부기관과 7개 국가가 참여하여 데이터셋 구축

Data Challenge Kaggle

WWW 2015의 Collocation workshop(Big 2015)에서 공유한 MS의 악성코드 dataset이 유명

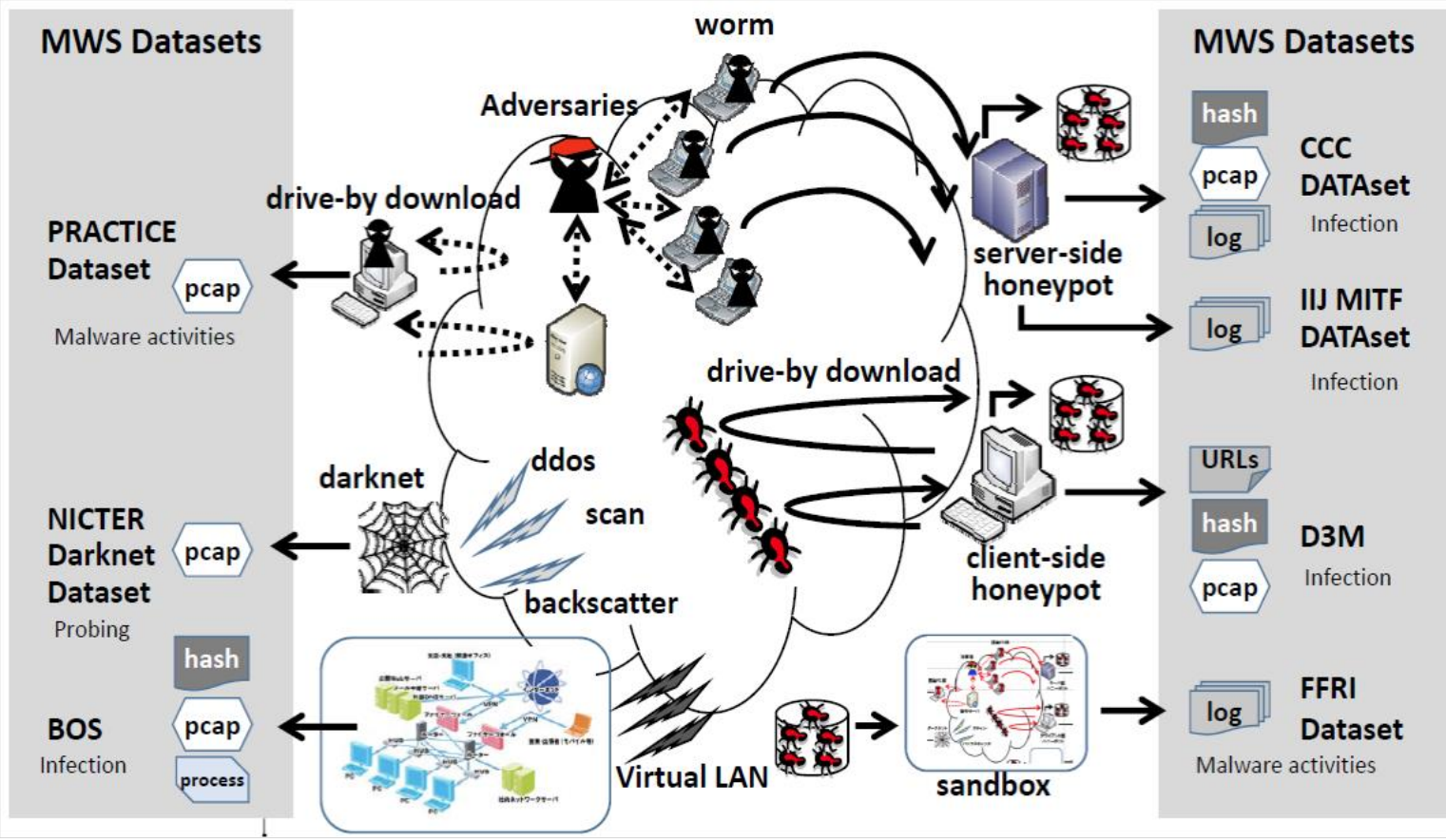
- 500G(10,868개) 악성코드 샘플
- 원본 악성코드 바이너리는 제공되지 않으며 1차 가공이 끝난 meta data가 제공됨





Data Challenge MWS(일본)

JPCERT/CC, IPA, AIST, NICT, 일본컴퓨터보안학회 주관 정보보안 데이터 분석 챌린지



MWS Dataset

	2008	2009	2010	2011	2012	2013	2014
CCC DATAset [server-side honeypot]	☑	☑	☑	☑	☑	☑	
MARS for MWS [malware dynamic analysis]	☑	☑	☑				
D3M [client-side honeypot]			☑	☑	☑	☑	☑
IIJ MITF DATAset [server-side honeypot]					☑		
PRACTICE Dataset [malware behavior analysis]						☑	
FFRI Dataset [malware sandbox analysis]						☑	☑
NICTER Darknet Dataset [darknet monitoring system]						☑	☑
Behavior Observable System (BOS) [observing threat actors]							☑

'08년 Server Honeypot 데이터 공유

'10년 Client Honeypot 데이터 추가

'13년 악성코드 행위 분석 결과 추가

'13년 다크넷 모니터링 데이터 추가

Data Challenge 한국

https://www.kisis.or.kr/kisis/subIndex/283.do

	자동형 악성코드	세인트시큐리티	2017 정보보호 R&D 데이터 챌린지 대회의 "악성코드 진제대응" 트랙에 활용된 [illegible]
악성코드 데이터셋	대용량 정상, 악성파일 1 (2017 예선)	한국인터넷진흥원, 하우리, 세인트시큐리티	2017 정보보호 R&D 데이터 챌린지 대회의 "악성코드 탐지" 트랙 예선에 활용된 15000개의 대용량 정상, 악성파일
	대용량 정상, 악성파일 2 (2017 본선)	한국인터넷진흥원, 하우리, 세인트시큐리티	2017 정보보호 R&D 데이터 챌린지 대회의 "악성코드 탐지" 트랙 본선에 활용된 15000개의 대용량 정상, 악성파일
	대용량 정상, 악성파일 3 (2018)	한국인터넷진흥원, 안랩, 이스트시큐리티, 하우리, 세인트시큐리티	2018 정보보호 R&D 데이터 챌린지 대회의 "AI기반 악성코드 탐지"에 활용된 50000개 악성코드
	VX Heaven 악성코드	호서대학교	VX heaven에서 배포하는, 15개의 악성코드 그룹으로 구성된 236,754개 악성코드
	메모리 상주 악성코드	한양대학교	실행파일 없이 메모리 상에 상주하는 악성코드 564개 및 분석 보고서
안드로이드 앱 데이터셋	정상/악성앱	고려대학교	다양한 악성앱 repository에서 수집한 9,990개의 악성앱 샘플과 109,193개의 정상앱
	오탐/제로데이 악성앱	고려대학교	Andro-Profiler에서 오진한 앱과 정상앱, 악성앱 샘플, Zero-day 앱 샘플을 포함하는 데이터셋
	대용량 악성·정상앱 1 (2018)	고려대학교	2018 정보보호 R&D 데이터 챌린지 대회의 "AI기반 안드로이드 악성 앱"에 활용된 14000개의 악성·정상 앱
차량 데이터셋	Car Hacking 데이터셋	고려대학교	DoS attack, fuzzy attack, spoofing the drive gear, spoofing the RPM gauge를 포함하는 자동차 해킹 데이터셋
	차량 이상징후 탐지	고려대학교	2017 정보보호 R&D 데이터 챌린지 대회의 "차량 이상징후 탐지" 트랙 본선에 활용된 정상 및 3종의 차량 공격시도 패킷 데이터
	차량 주행 데이터 (2018)	고려대학교	2018 정보보호 R&D 데이터 챌린지 대회의 "차량 주행 데이터 기반 도난 탐지"에 활용된 700km 차량 주행 데이터

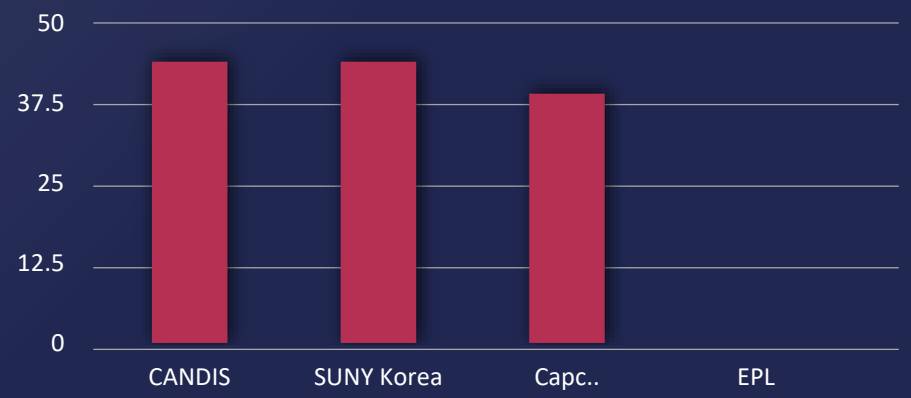
스크린샷

Data Challenge KISA, 고려대학교 운영(2017, 2018)

정보보호 R&D 데이터 챌린지(2017.12.8)

[2차 데이터셋 분석]

CANDIS	SUNY KOREA	CAPCORPSCERT0188	EPL
44.736…	44.736…	39.394	0.0



현재시각 : 12:42:16

차량 이상징후 탐지

팀명	1차(탐지 정확도)	2차(탐지 정확도)
CANDIS	89.474	0.0
SUNY Kor..	89.474	0.0
Capcor..	78.788	0.0
EPL	0.0	0.0
-		
-		
-		

2018년 인공지능 기반 악성앱 탐지

2018 AI기반 안드로이드 악성앱 탐지 트랙

- AI/ML을 이용한 Android App 분류/진단은 데이터 분석 기반 보안 분야(data-driven security)의 대표적인 응용 사례

악성앱 데이터셋(Andro-Profiler dataset)

- 관련 논문(Citation : 30+)
  - Jang, Jae-wook, et al. "Detecting and classifying method based on similarity matching of Android malware behavior with profile." SpringerPlus 5.1 (2016): 273.
  - Jang, Jae-wook, et al. "Andro-profiler: anti-malware system based on behavior profiling of mobile malware." Proceedings of the 23rd International Conference on World Wide Web. ACM, 2014.
- 인용한 주요 논문 예 :
  - Feizollah, Ali, et al. "A review on feature selection in mobile malware detection." Digital investigation 13 (2015): 22-37.
  - Neal, Tempestt J., and Damon L. Woodard. "Surveying biometric authentication for mobile device security." Journal of Pattern Recognition Research 1 (2016): 74-110.

악성앱 데이터셋(Andro-Profiler dataset)

- Original dataset: http://ocslab.hksecurity.net/andro-profiler
- Description (예선): http://datachallenge.kr/challenge18/malware/introduction/
- 예선/본선 데이터셋 및 정답지 등: http://ocslab.hksecurity.net/Datasets/datachallenge2018/android

2018년 예선/본선 총평 안드로이드 악성앱 트랙

안드로이드 악성앱 트랙

2017년에 비해 전반적인 레벨 상승

- 7팀이 90% 이상 정확도를 보임 (예선)
- 9팀이 87% 이상 정확도를 보임 (예선)

악성앱의 자동분석은 이제 보편적인 수준의 기술이 되었음

- **과거에는 데이터셋 sample을 구하기 어려운 점, 예제 코드가 없던 점이 주요 허들이었음**
- **현재는 python의 다양한 library 및 예제코드, 동영상 강의, 데이터셋 sample이 존재**

전년 Deep learning을 적용한 팀 수 증가

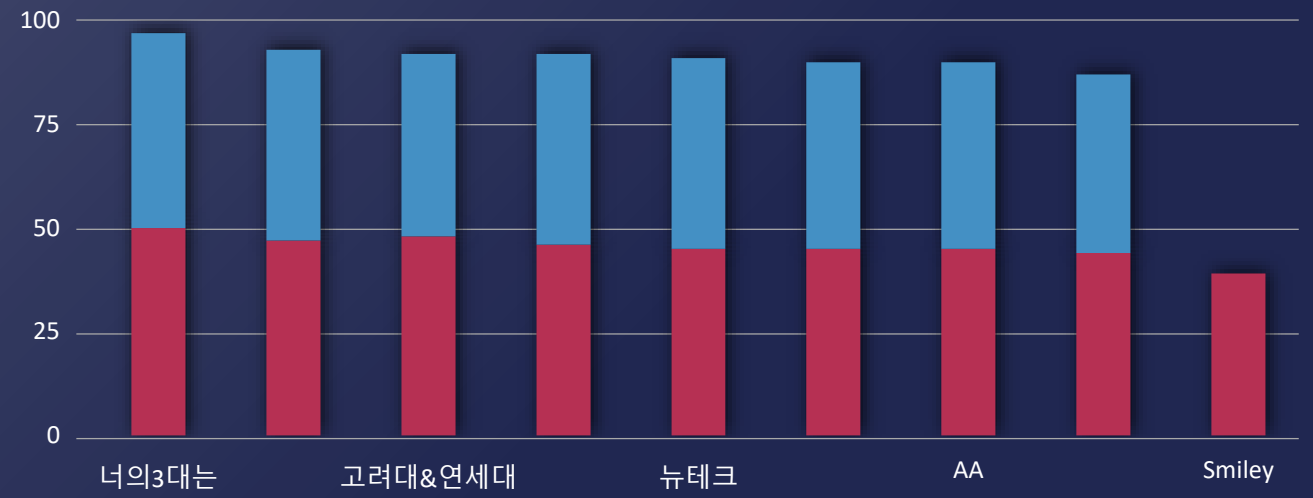
- 기계적으로 알고리즘들을 적용을 한 것인지, 목표를 뚜렷이 하여 feature engineering을 하였는지 불분명한 팀들이 많음
- 단순 trial&error 형태의 deep learning node/layer 개수 구성 및 activation function(ReLu, Sigmoid, …) 선정 보다는 그렇게 구성한 근거까지 제시하지는 못한 팀들이 많음

정보보호 R&D 데이터 챌린지 2018 본선대회

2018-12-01 / 21:03:58

AI기반 안드로이드 악성앱 탐지

너의3대는?	유홍렬	고려대&연세대	MLCS	뉴테크	노위캔	AA	한명이사라졌어요	Smiley
97.53%	95.85%	94.33%	94.23%	93.95%	91.38%	89.33%	87.6%	39.08%



AI기반 안드로이드 악성앱 탐지

팀명	1차(탐지 정확도)	2차(탐지 정확도)
너의3대는?	97.4%	97.65%
유홍렬	94.4%	97.3%
고려대&연세대	95%	93.65%
MLCS	92.15%	96.3%
뉴테크	91.5%	96.4%
노위캔	92.1%	90.65%
AA	90%	88.05%
한명이사라졌어요	88.55%	86.65%
Smiley	78.15%	0%

CAVEATS: AI 기반 악성코드 탐지

Academic paper/research의 동향과 현업의 동향은 다름

- Model maintenance 까지 제대로 고려한 논문들은 무척 적음

- 초기 탐지 알고리즘은 제안하지만,
  실제로 지속적인 모델링과 업데이트까지 고려하지 않은 경우가 많음

- 현업에서 원하는 점은 지속적인 model maintenance cost를 낮추는 것
  - T, t+1, t+2… 로 time window 가 sliding 될 때 점차 탐지율이 떨어지는지를 모니터링해서 재학습을 자동으로 유도하는 모델 (예: EWMA algorithm) 까지 고려해야 함

CAVEATS:AI 기반 악성코드 탐지

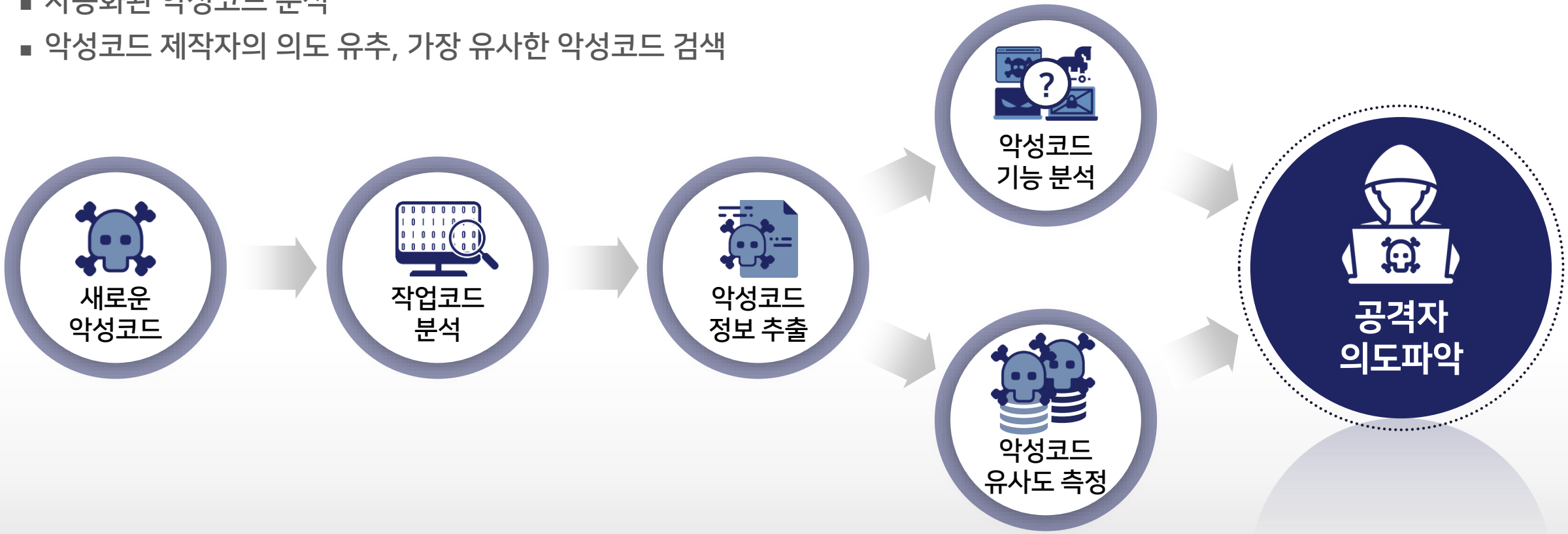
- 특정 feature 기반 분류는 여전히 유효하지만 악성앱들이 진화하면서 유효성이 떨어져가고 있음
  - 예1 : Permission based detection - 최근에는 정상앱이나 악성앱이나 과도한 Permission을 요구하는 경향이 있음
  - 예2 : API call sequence - 과거에는 그 자체로 결정적인 feature였으나 지금은 one of features가 됨

- Classical ML(random forest, artificial neural network…)을 이용한 악성앱 탐지(Android 기반)
  그 자체는 이미 보편적인 기술로 많은 조직들에서 자체적으로 개발하여 쓰고 있음
  - Deep learning을 활용하는 것이 한계를 뛰어넘을 수 있는 방법
  - 단, 현업에서는 아직 deep learning에 대한 의구심은 있음

지능적 악성코드 탐지시스템 개발사례

Cyber Genome

- 자동화된 악성코드 분석
- 악성코드 제작자의 의도 유추, 가장 유사한 악성코드 검색

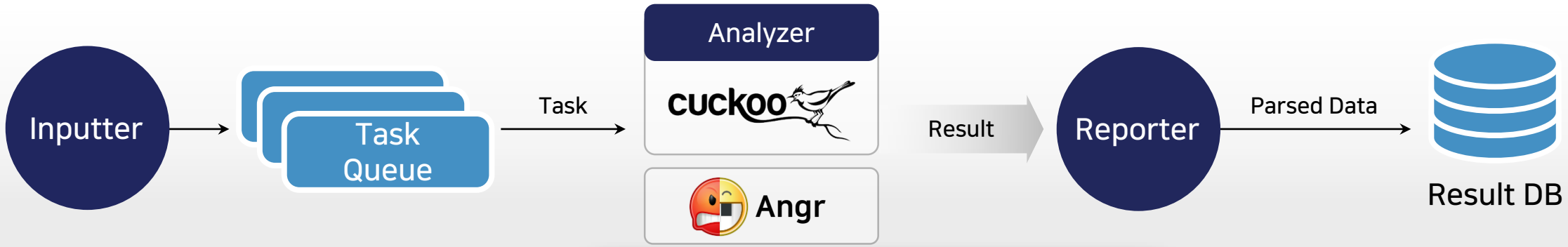


새로운 악성코드에 대한 공격자 의도 파악 흐름도

악성코드 분석 시스템 – architecture

악성코드 분석 시스템 architecture

- Inputter : 악성코드를 분석 큐에 순차적으로 넣어주는 입력 모듈
- Analyzer : 악성코드의 정적/동적 분석을 수행하는 모듈
  - Cuckoo : 악성코드 분석 자동화를 위한 오픈소스 샌드박스
  - Angr : python 기반의 바이너리 분석 프레임워크로 바이너리 파일의 Control Flow Graph를 생성하는데 이용
- Reporter : Analyzer가 분석한 악성코드 정보를 summary하여 DB에 적재하는 모듈
- 웹 대시보드 : DB에 적재된 악성코드 현황, Analyzer 상태 확인, 악성코드 분석 정보 조회/검색

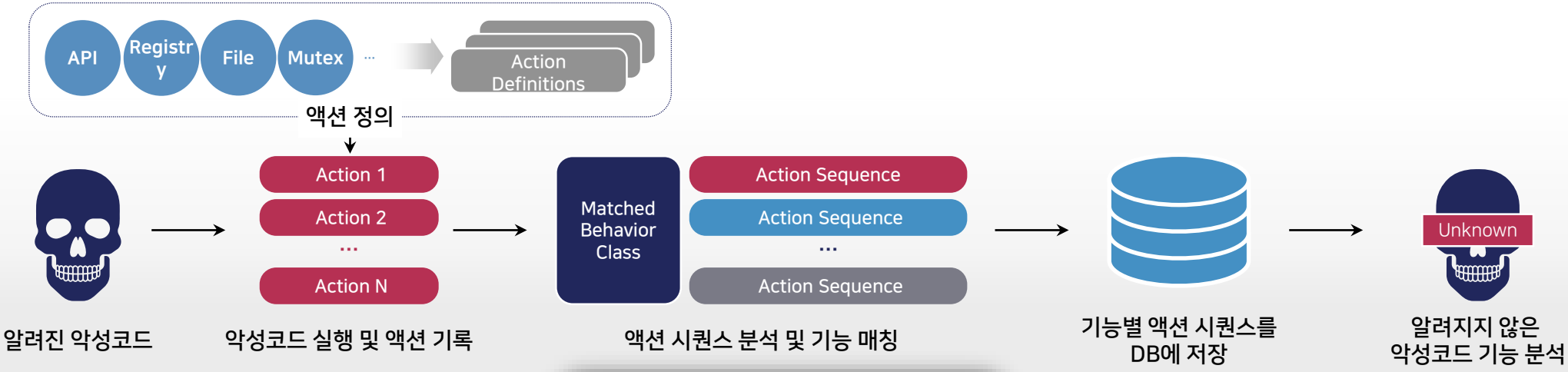


악성코드 분석 시스템 architecture

악성코드의 기능(function) 중심 분석

악성코드의 기능 중심 분석

- 악성코드의 동적 정보 (API 콜, 레지스트리, 파일 등)를 중심으로, 악성코드의 액션을 정의
  - 악성 행위로 의심되는 API 콜, 레지스트리 접근, 파일 등을 탐지 조건으로 두어 액션을 정의함
- **악성코드의 유사도 파악 및 해커의 의도를 파악할 수 있음**
- 악성코드 분석 시스템에서 추출된 액션 시퀀스 정보를 바탕으로 악성코드 기능 분석 진행
  - 액션 시퀀스는 악성코드가 실행되면서 위에서 정의한 액션이 시퀀스로 기록된 것으로 악성코드의 동적 행동을 나타냄



악성코드의 기능(function) 중심 분석

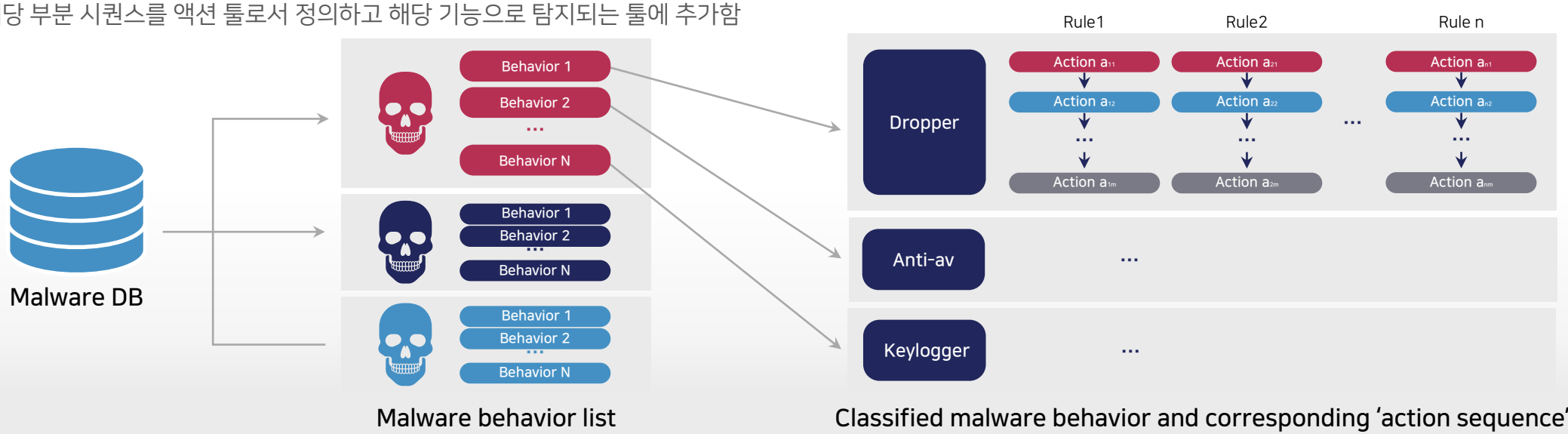
악성코드의 기능 분석

- 기능별 액션 시퀀스 분석
  - 알려진 샘플을 이용하여 악성코드 기능에 따라 나타나는 액션 시퀀스를 정의함

    액션 시퀀스 내에서 자주 등장하는 부분 시퀀스를 분석

    해당 부분 시퀀스가 악성코드의 어떤 기능에 해당될지 액션의 정의를 통해 확인

    해당 부분 시퀀스를 액션 툴로서 정의하고 해당 기능으로 탐지되는 툴에 추가함



API 액션 룰 정의

악성코드의 기능(function) 중심 분석

악성코드 주요 기능

▪ 탐지하고자 한 악성코드의 주요 기능 15가지를 도출

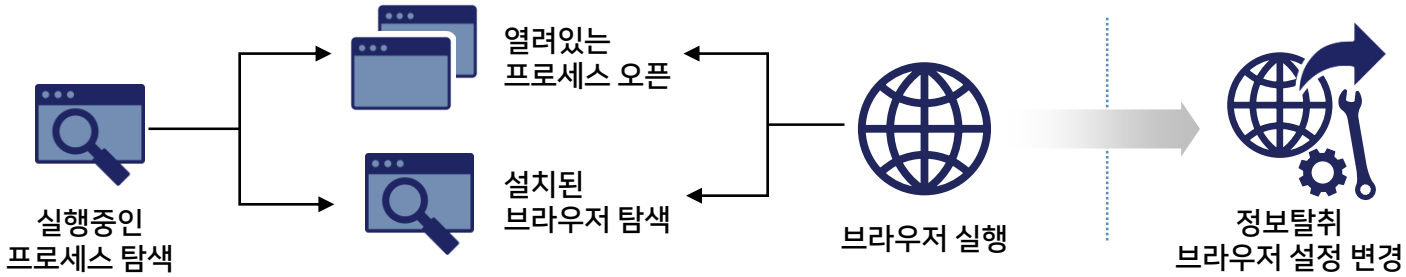
No.	악성코드 기능	내용	No.	악성코드 기능	내용
1	Adware	사용자의 동의 없이 광고를 띄우는 프로그램으로 브라우저를 실행하고 설정을 변경하는 기능	9	Downloader	외부로부터 악성코드를 다운로드하여 장비를 감염시키는 기능
2	Anti-AV	백신 프로그램을 탐지한 후 우회 및 종료 시키는 기능	10	Dropper	실행가능한 바이너리 파일을 설치 및 실행하는 기능
3	Anti-debug	디버깅을 방지하는 기능	11	Info Stealer	레지스트리나 파일을 이용해 인터넷 브라우저나 ftp 프로그램 등에 저장된 개인 정보를 탈취
4	Anti-sandbox	악성코드 자신이 실행되는 환경이 샌드박스인지 확인하는 기능	12	Keylogger	키보드 입력 이벤트를 후킹하여 정보를 외부로 유출시키는 기능
5	Backdoor	일반적인 인증과정을 거치치 않고 권한을 획득하여 악성 행위를 하는 기능	13	Ransomware	사용자의 파일을 암호화하여 복호화를 위한 개인 키의 대가로 돈을 받음
6	Botnet	사용자의 컴퓨터를 bot으로 만들고 네트워크 연결을 통해 원격 접근과 통제를 가능하게 함	14	Stealth	악성 행위를 은폐함으로써 사용자에게 자신을 드러나지 않게 하는 기능
7	Code Injection	기존 프로세스에 악성 코드를 주입하여 공격자가 권한을 얻거나 원하는 행동을 취함	15	Worm	자신을 복제하여 네트워크 상에 전파시켜 다른 장비를 감염시키는 기능
8	Destroy MBR	하드디스크의 Master Boot Record 영역을 비정상적인 값으로 변경하는 기능	-	-	-

악성코드 기능

악성코드의 기능(function) 중심 분석 주요기능 예시

Adware

- 사용자의 동의 없이 광고를 띄우는 프로그램으로 브라우저를 실행하고 설정을 변경
- 기능 액션 시퀀스
  - Adware 설치 및 웹 브라우저를 열기 위한 행위 진행 후 정보 탈취나 브라우저 설정을 변경함

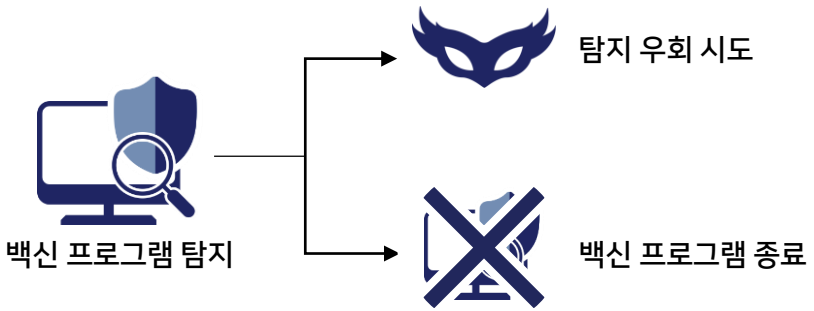


액션	탐지된 행위 정보	설명
실행중인 프로세스 탐색	injection_process_search	Process32FirstW, Process32NextW를 이용해 실행 중인 프로세스 확인
프로세스 오픈	process_needed	이미 브라우저 process가 오픈되어 있는 경우 브라우저 오픈
설치된 프로그램 탐색	queries_program	현재 설치되어 있는 브라우저 검색
브라우저 실행	locates_browser	Chrome, Firefox 등의 인터넷 브라우저를 실행
정보탈취	infostealer_browser	브라우저를 통해 생성된 파일이나 레지스트리 키를 접근
브라우저 설정 변경	modifies_browser_configuration	NtWriteFile로 브라우저의 profile을 재생성
브라우저 통신 비활성화	disables_spdy_browser, disables_browser_http2	브라우저 내 SPDY 통신이나 HTTP 2.0 통신을 비활성화

악성코드의 기능(function) 중심 분석 주요기능 예시

Anti-AV

- 백신 프로그램을 탐지한 후 우회, 종료 시키는 기능이 있는 악성코드
- 기능 액션 시퀀스
  - 백신 프로그램 존재 여부를 탐지한 후 발견 후에 프로세스 이름을 변경해 우회하거나 해당 백신 프로그램을 종료시킴



액션	탐지된 행위 정보	설명
레지스트리 키를 통한 AV 설치 확인	antiav_detectreg	레지스트리키를 이용해 알려진 AV의 설치 여부 확인
설치된 파일을 통한 AV 설치 확인	antiav_detectfile	설치된 파일 정보를 이용해 알려진 AV의 설치 여부 확인
알려진 AV 라이브러리 탐지	antiav_avast_libs	LdrLoadDll, LdrGetDllHandle 모듈을 이용해 알려진 AV 라이브러리 탐지
원격 프로세스 종료	terminates_remote_process	다른 프로세스를 원격으로 종료
서비스 종료	antiav_servicestop	OpenServiceW, ControlService 콜을 통해 활성 상태의 서비스를 종료
알려진 프로세스 명 변경	stealth_system_procname	프로세스 명을 널리 알려진 프로세스 명으로 변경

악성코드의 기능(function) 중심 분석 주요기능 예시

Anti-Sandbox

- 악성코드 자신이 실행되는 환경이 샌드박스인지 확인함
- 기능 액션 시퀀스
  - 샌드박스가 갖는 특수성을 이용해 샌드박스 환경을 감지하고 악성코드 분석을 방해함

샌드박스 관련 파일 검색

포그라운드 창 검사

Idle 시간 검사

프로세스 지연

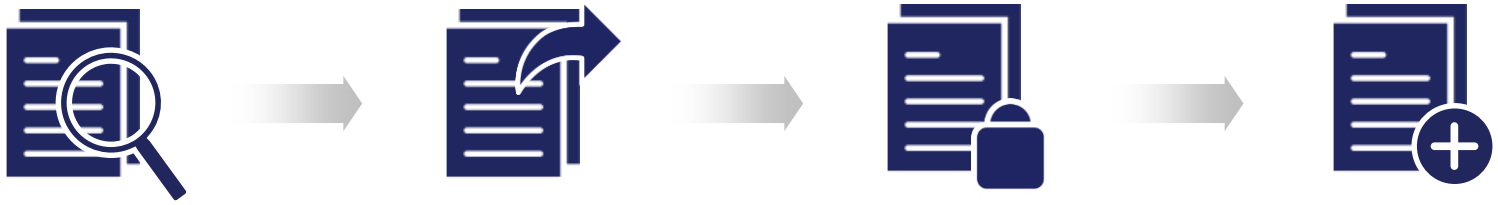
관련 API 언후킹

액션	탐지된 행위 정보	설명
Anti-sandbox	antisandbox_cuckoo_files	쿠쿠 샌드박스 환경에만 존재하는 디렉토리를 탐지함
	antisandbox_foregroundwindows	GetForegroundWindow와 NtDelayExecution 함수를 사용하여 유저가 포그라운드에서 실행되는 윈도우 창을 사용하는지 지속적으로 탐지
	antisandbox_idletime	NtQuerySystemInformation의 첫번째 인자로 SystemProcessofrPerformanceInformation을 전달하여 윈도우의 idle 시간을 탐지함
	antisandbox_sleep	NtDelayExecution 함수를 사용하여 프로세스를 지연시켜 분석을 방해함
	antisandbox_unhook	쿠쿠 샌드박스가 모니터링하는 함수를 언후킹함

악성코드의 기능(function) 중심 분석 주요기능 예시

Ransomware

- 사용자의 파일을 모두 암호화하여 이후 복호화를 위한 개인 키를 알려주는 대가로 돈을 받음
- 기능 액션 시퀀스
  - 목표 파일을 찾아 파일을 이동시켜 암호화 한 후, 파일을 새로 생성함



목표 파일 탐색 → 파일 이동 → 파일 암호화 → 파일 생성

액션	탐지된 행위 정보	설명
목표 파일 탐색	FindNextFile, FindFirstFileEx	해당 디렉토리에서 존재하는 파일을 모두 탐색
파일 이동	ransomware_file_moves	MoveFileWithProgress API를 통해 목표 파일 이동
파일 암호화	SetFileAttributes	파일 속성을 "ENCRYPTED"로 변경
파일 생성	ransomware_appends_extensions	새로운 확장자명을 가진 파일로 변경
	CreateFile, CopyFile	새로운 확장자명을 가진 파일 생성

악성코드 유사도 측정 API 콜 시퀀스 기반 유사도 측정

API 콜 시퀀스 유사도 측정

- API 콜 시퀀스를 이용한 유사도 측정
  - 악성코드의 동적 행동을 보여주는 API 콜 시퀀스를 이용하여 동적 유사도 측정
  - Nilsimsa 와 같은 similar 알고리즘의 한계점을 개선하여 적용

Trojan-Ransom.Win32.Wanna.b

P1 - GetComputerNameW, RegCreateKeyExW,
P2 - GetSystemTimeAsFileTime, SetUnhandledExceptionFilter,
P3 - FindFirstFileExW, NtDelayExecution, GetTempPathW,
P4 - GetSystemTimeAsFileTime, NtClose, NtOpenKey

P1 P2 P3 P4

1f539595330436fd7d0179dd8251d20c211c0099a6508345dcad311083055a91

Trojan-Ransom.Win32.Wanna.zbu

Q1 - GetSystemTimeAsFileTime, SetUnhandledExceptionFilter,
Q2 - GetSystemTimeAsFileTime, NtClose, NtOpenKey,
P3 - FindFirstFileExW, NtDelayExecution, GetTempPathW,
Q4 - GetComputerNameW, RegCreateKeyExW,

Q1 Q2 Q3 Q4

1f539595830436fd7d0179dd8251d20c211c0099a4c08345dc8c311083055a91

0. 96875

[API 콜 시퀀스 유사도 측정 예시]

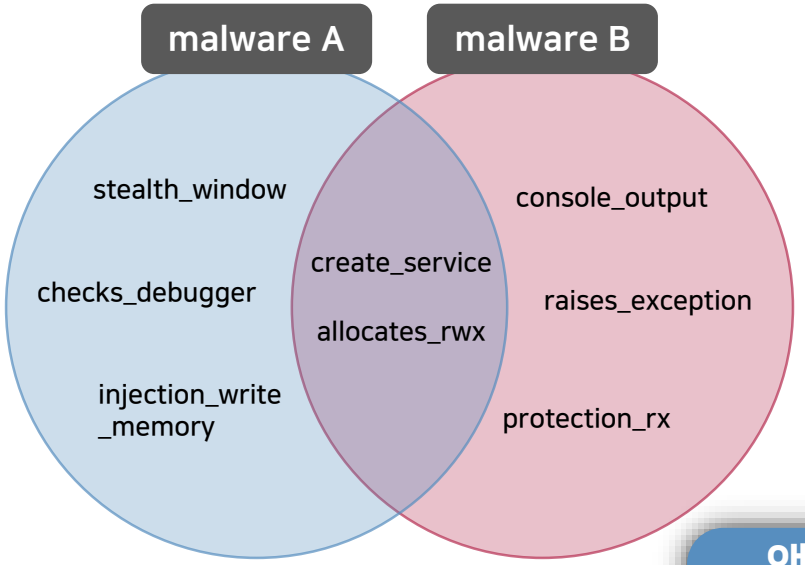
악성코드 유사도 측정 액션 집합 기반 유사도 측정

액션 유사도 측정

- 기능 분석 시 추출한 액션을 활용하여 각 악성코드의 액션 집합끼리 유사도 측정
  - Jaccard Similarity 사용 - 집합 간 유사도 측정
  - 예시

    malware A가 가진 액션 : stealth_window, create_service, checks_debugger, injection_write_memory, allocates_rwx

    malware B가 가진 액션 : create_service, allocates_rwx, console_output, raises_exception, protection_rx



Jaccard Similarity

$$|A \cap B| = 2$$
$$|A \cup B| = 8$$
$$\frac{|A \cap B|}{|A \cup B|} = 0.25$$

액션 유사도 측정 예시

CONCLUSION REMARK

AI를 활용한 악성코드 탐지

- AI + Security의 목적으로 국내외에서 dataset 공유가 활발히 이루어지고 있음

- 지난 2년간 정보보호 데이터 R&D 챌린지 대회 운영을 통해 확인한 결과,
  악성코드, 악성앱, 침입탐지 등 다양한 분야에 AI+Security가 적용될 수 있음을 검증
  - 전문 보안기업과 대학간 활발한 교류 필요성의 증대

- AI + Security는 매우 promising한 분야로 기술 선점이 중요

AI를 활용한 악성코드 탐지

- 기 SDS 내에서 AI를 활용하여, SIEM 운영 효율화 및 악성코드 탐지에 적극 활용 중
- 악성코드(malware) 분석 + CTI(Cyber Threat Intelligence)로의 확대
- 양질의 dataset 구축을 하기 위해 지속적인 노력 필요

Thank you