기존 백신의 한계점을 극복하는 다중 AI 백신 플랫폼(요약)

성과Track	기초·미래선도	산업육성	국가·사회문제해결
			17.사이버 범죄

협약(세부)과제명	지능화된 악성코드 위협으로부터 ICT 인프라 보호	
과제번호	협약(세부) 과제번호	NTIS 과제번호
	2019-0-00026	
성과목표	기존 백신의 한계점을 극복하는 다중 AI 백신 플랫폼 개발	
총 연구기간	2019년 4월 1일~ 2022년 12월 31일	
총 연구비	총 6,031 백만원	정부: 4,901 백만원 민간: 1,130 백만원

연구책임자	연구자 성명	직할부서	연구본부/연구실	직위/직급
	김종현	지능화융합연구소	정보보호연구본부/ 네트워크·시스템보안연구실	기술총괄/책임

성과 정보

성과 내용	ㅇ **(시범서비스)** ETRI 융합기술생산연구센터 입주기업에 **다중 AI 백신 시범 적용/운영**(~'22.05) ㅇ **(국방 실증)** 국방 인공지능 백신체계 개발을 위한 **국방분야 AI백신 실증/성능검증 완료**(~'22.09) ㅇ **(공인시험 검증)** 성능평가의 객관성 확보를 위한 **국가공인시험 인증서 획득**('22.10) ㅇ **(국방 ISP사업)** 軍에 특화된 인공지능 백신체계 구축을 위한 **ISP 사업의 성공적인 수행**(~'21.12) ㅇ **(학술적 검증)** 비실행형 악성코드 탐지 기술에 대한 **SCI 논문 6.5건 게재** 및 신뢰성 확보 ㅇ **(표준화)** ITU-T SG17 **국제표준 1건**(ITU-T X.1218) 제정 및 TTA PG503 **국내표준 3건** 제정 ㅇ **(사업화)** 악성코드 및 위협 정보 대응 Feed-Service **사업화 2건 달성** 및 **국방 u-실험사업 지원** ㅇ **(기술 개발)** 2022년도 ICT R&D 우수과제 및 **우수연구자(IITP 원장상) 수상**('22.11)

정량성과		논문		특허				기술이전	
	기본지표	SCI(건)	비SCI(건)	해외(건)		국내(건)		건수	금액 (백만원)
				출원	등록	출원	등록		
		6.5	24.5	5	2	13	4	3	77

정량성과	심화지표	표준화된 IF 상위 20% SCI 논문(건)	특허활용률 (기술이전건수/특허등록보유건수)	국제표준승인표준 기고서(건)	3극 특허(건)	연구비 대비 기술료 수입(%)
		1	100 %	1	0	1.3

대표성과 1	ㅇ **(학술적 검증)** 비실행형 악성코드 탐지 기술 등에 대한 <u>다수의 SCI 논문 게재 및 특허 등록</u> - 대표논문: Evaluations of AI-based Malicious PowerShell Detection with the Feature Optimizations, 송지현 외, ETRI 저널, Vol 43, No. 3, IF 1.347, 2021년 6월 - 대표특허: PACKER CLASSIFICATION APPARATUS AND METHOD USING PE SECTION INFORMATIONS, US11,429,819, 2022년 8월, 미국, 등록
대표성과 2	ㅇ **(실효성 검증)** ETRI AI백신기술의 실효성 검증을 위한 <u>민간 시범서비스 및 국방 실증/성능검증 완수</u> - 시범서비스 : **보안 사각지대 해소**를 위한 중소기업 대상 **클라우드 AI백신 시범서비스** 추진('21.05~'22.05) - 국방실증 및 ISP사업 : 軍 내부 사이버망(국방망)에서 **ETRI AI백신기술 적용 및 성능검증**을 통한 AI백신 국방실증 및 ISP사업 수행으로 **'24년도 국방부 인공지능 백신체계 구축사업 추진 확정**

2022년도 ETRI 10대 대표성과 후보 추천서(상세)

1. 성과명

기존 백신의 한계점을 극복하는 다중 AI 백신 플랫폼

2. 성과내용

기술개발 목표달성도

□ 기술적 선점이 필요한 분야

○ 現 상용 백신 솔루션의 한계점*을 극복하고, 주요 ICT 인프라의 마비 사태를 막을 수 있는 클라우드 기반 **다중 AI 백신 플랫폼** 분야

* 신종 악성코드 실시간 처리 불가, 시스템 리소스 부족, 이기종 백신간 호환성 문제 등

○ 고도화되고 있는 최신 악성코드 공격으로부터 국방 핵심 인프라를 보호할 수 있는 **軍에 특화된 인공지능 백신체계 구축을 위한 AI 백신 기술** 분야

□ 기술개발 목표

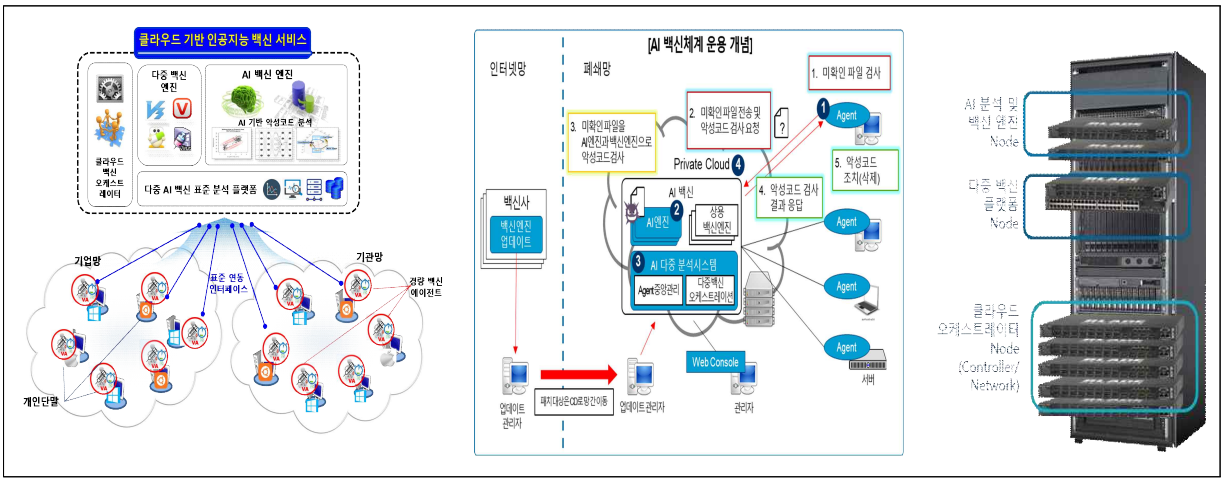
○ 지능화된 악성코드를 이용한 사이버공격으로부터 ICT 자원을 보호할 수 있는 **클라우드 기반 경량 공통 백신 에이전트 및 AI 다중 백신 분석 시스템 개발**

(목표 ①) 이종 백신 간 호환성 문제 해결을 위한 **경량 AI 백신 에이전트 기술**

(목표 ②) 다중 백신 통합 운영(**클라우드 오케스트레이션**)을 위한 **다중 AI 백신 분석 플랫폼**

(목표 ③) 변종/신종 악성코드 탐지 및 대응을 위한 **인공지능 악성코드 분석 기술**

<기술개발 개념도>



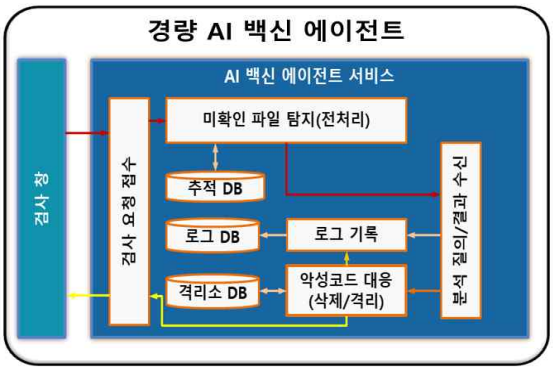
□ 기술개발 목표의 달성 성과 및 핵심기술 확보

[개발목표 ①] 이종 백신 간 호환성 문제 해결을 위한 경량 AI 백신 에이전트 기술

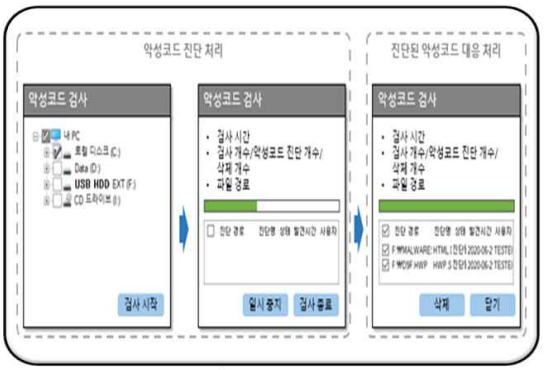
➡ (달성성과) Windows 및 리눅스 단말용 경량 공통 백신 에이전트 개발

➡ (핵심기술 확보)

- 초경량의 공통 백신 에이전트 기술
- 실시간 파일 필터 및 자체 보호 기술을 통한 에이전트 보호 기술 개발
- 다중 백신 분석 플랫폼과의 표준 인터페이스 및 프로토콜 개발



• 경량 AI 백신 에이전트의 분석처리 모듈 구성도



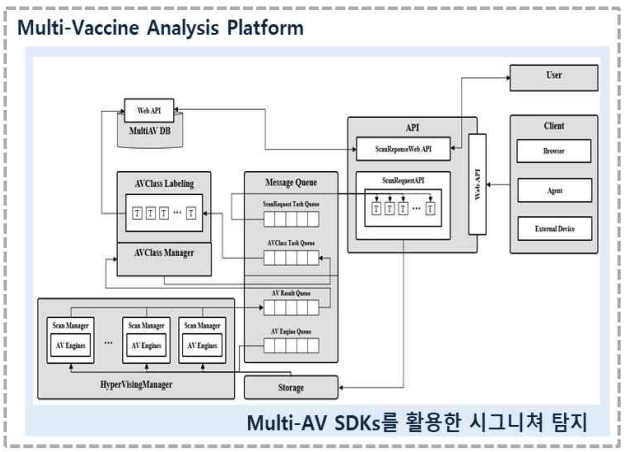
<리눅스용 GUI 모듈>

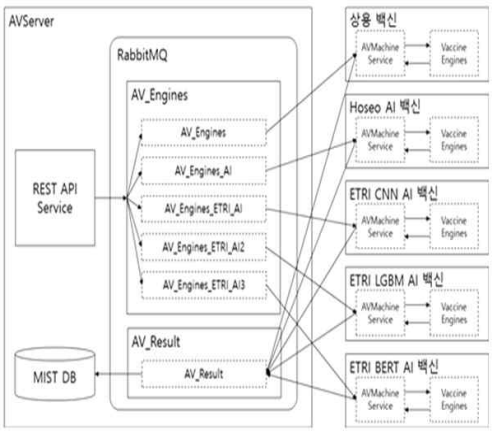
[개발목표 ②] 클라우드 기반 다중 AI 백신 분석 플랫폼 기술

➡ (달성성과) 다중 백신 및 AI 백신의 진단 및 분석을 이용한 악성코드 탐지 종합 진단 알고리즘 개발

➡ (핵심기술 확보)

- 다중 백신 분석 결과를 이용한 악성코드 탐지명 표준화 기술 개발
- 다중 백신 및 AI백신을 위한 서비스 오케스트레이터 기술 개발
- 정책 기반 백신 에이전트 소프트웨어 및 패턴 업데이트 관리 기능 개발





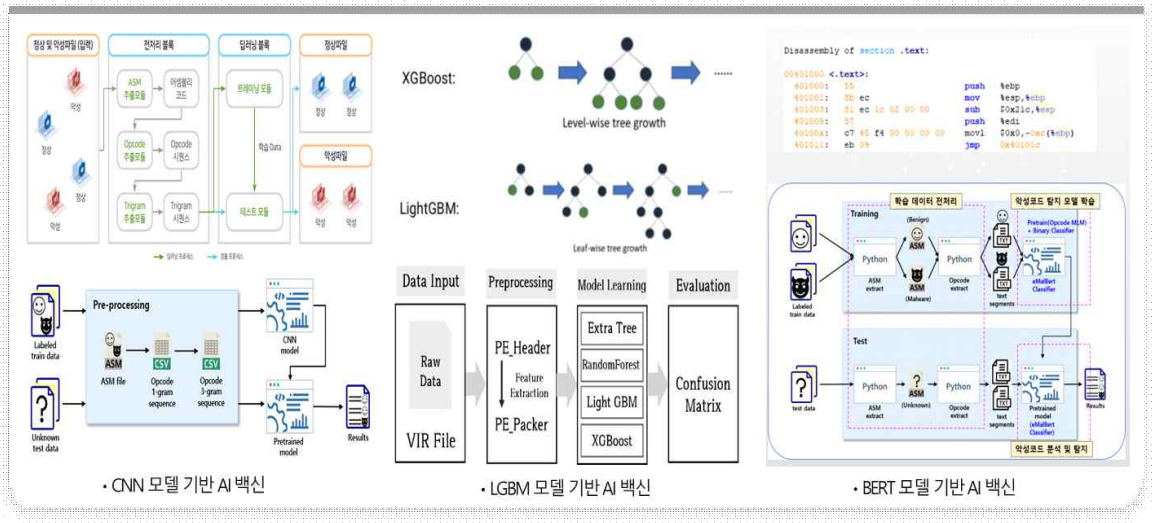
• 상용 백신 및 AI백신 연동 구조도

[개발목표 ③] 변종/신종 악성코드 탐지 및 대응을 위한 AI 악성코드 분석 기술

➡ (달성성과) PE, Fileless, 문서형 파일에 대한 AI 악성코드 분석 기술

➡ (핵심기술 확보)

- 앙상블 기반 지능형 다중 AI 학습 알고리즘 및 탐지 엔진 개발
- Fileless 악성코드 탐지 기술 개발
- HWP 기반 문서형 악성코드 분석 기술 개발

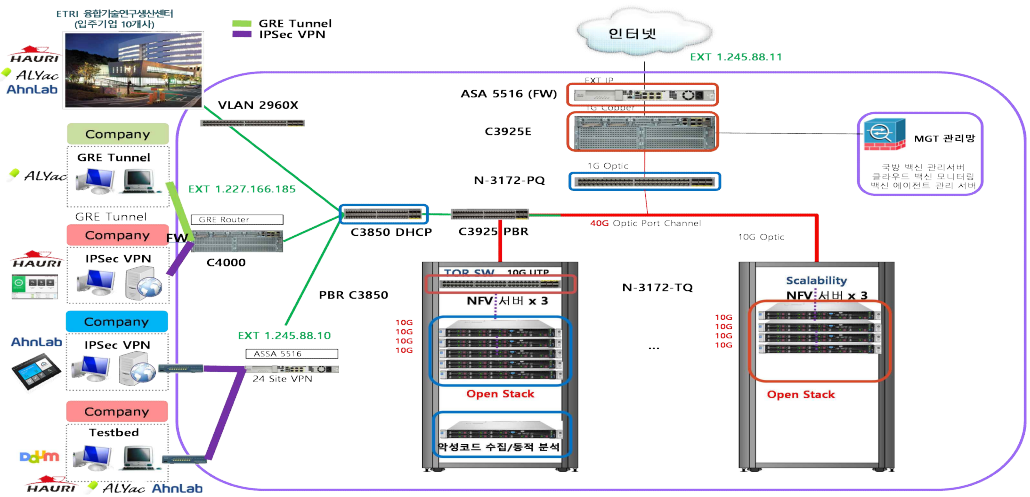


3. 우수성 및 차별성

기술수준 향상 성과

○ (시범서비스) 클라우드 기반 AI 백신 기술의 민간 실증을 위한 시범서비스 운영('21.05~'22.05)

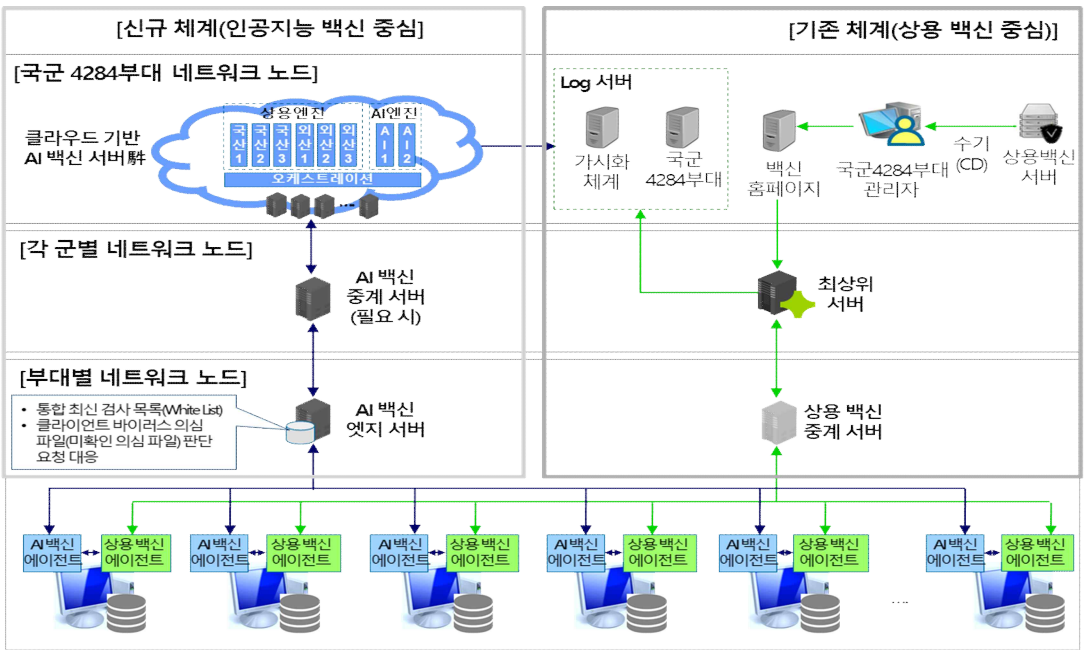
- 클라우드 기반의 오케스트레이션 기술, 다중분석 플랫폼, 다중백신 및 AI 백신 기술을 활용
- ETRI 융합기술연구생산센터 입주 6개 중소기업 대상 사이버해킹테스트베드 기반 실증



< 클라우드 다중 AI 백신 시범서비스 구성도 >

○ (국방 ISP 사업) 국방 인공지능 백신체계 ISP 사업 수주 및 성공적인 수행('20.06~'20.12)

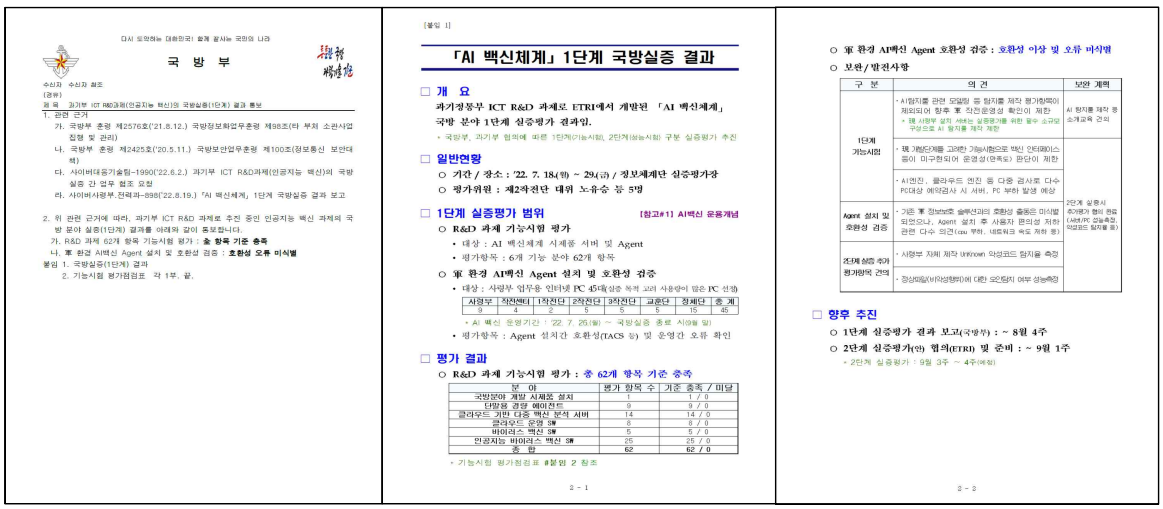
- 국방 인공지능 백신체계 개발을 추진하기 위하여 단기 구축계획 및 중장기 로드맵을 마련하기 위한 ISP 사업 수행



< 국방 ISP 사업을 통해서 제안한 신규 인공지능 백신체계 >

○ (국방 실증) ETRI AI백신 기술의 유효성 검증을 위한 국방 실증 완료('22.05~'22.09)

- 국방부, 과기부 협의에 따라 1단계(기능시험), 2단계(성능시험) 구분하여 실증 시험평가 추진
- 1단계 실증결과: R&D 수행과제의 62개 기능 항목에 대한 시험평가 결과(전 항목 합격판정)를 국방부 보고('22.07.18~'22.07.29)
- 2단계 실증결과: AI백신 성능시험 및 국방 인터넷망 적용/운영 보고('22.09.14~'22.09.23)



다시 도약하는 대한민국! 함께 잘사는 국민의 나라

국 방 부

수신자 수신자 참조

(경유)

제 목 과기부 ICT R&D과제(인공지능 백신)의 국방실증(1단계) 결과 통보

1. 관련 근거

가. 국방부 훈령 제2576호('21.8.12.) 국방정보화업무훈령 제88조(타 부처 소관사업 접형 및 관리)

나. 국방부 훈령 제2425호('20.5.11.) 국방보안업무훈령 제100조(정보통신 보안대책)

다. 사이버대응기술팀-1990('22.6.2.) 과기부 ICT R&D과제(인공지능 백신)의 국방 실증 간 업무 협조 요청

라. 사이버사령부-전략과-998('22.8.19.) 「AI 백신체계」 1단계 국방실증 결과 보고

2. 위 관련 근거에 따라, 과기부 ICT R&D 과제로 추진 중인 인공지능 백신 과제의 국방 분야 실증(1단계) 결과를 아래와 같이 통보합니다.

가. R&D 과제 62개 항목 기능시험 평가 : **全 항목 기준 충족**

나. **軍 환경 AI백신 Agent 설치 및 호환성 검증 : 호환성 오류 미식별**

붙임 1. 국방실증(1단계) 결과

2. 기능시험 평가점검표 각 1부. 끝.

[붙임 1]

「AI 백신체계」 1단계 국방실증 결과

□ 개 요

과기정통부 ICT R&D 과제로 ETRI에서 개발된 「AI 백신체계」 국방 분야 1단계 실증평가 결과임.

◦ 국방부, 과기부 협의에 따른 1단계(기능시험), 2단계(성능시험) 구분 실증평가 추진

□ 일반현황

○ 기간 / 장소 : '22. 7. 18.(월) ~ 29.(금) / 정보체계단 실증평가장

○ 평가위원 : 제2작전단 대위 노유승 등 5명

□ 1단계 실증평가 범위 [참고#1] AI백신 운용개념

○ R&D 과제 기능시험 평가

• 대상 : AI 백신체계 시제품 서버 및 Agent

• 평가항목 : 6개 기능 분야 62개 항목

○ 軍 환경 AI백신 Agent 설치 및 호환성 검증

• 대상 : 사령부 업무용 인터넷 PC 45대(실증 목적 고려 사용량이 많은 PC 선정)

사령부	작전센터	1작전단	2작전단	3작전단	교육단	정제단	총 계
3	4	2	5	5	5	15	45

• AI 백신 운영기간 : '22. 7. 25.(월) ~ 국방실증 종료 시(9월 말)

• 평가항목 : Agent 설치간 호환성(TACS 등) 및 운영간 오류 확인

□ 평가 결과

○ R&D 과제 기능시험 평가 : 총 62개 항목 기준 충족

분 야	평가 항목 수	기준 충족 / 미달
국방분야 계량 시제품 설치	1	1 / 0
단말용 경량 에이전트	9	9 / 0
클라우드 기반 대용 백신 분석 서버	14	14 / 0
클라우드 운영 SW	8	8 / 0
바이러스 백신 SW	5	5 / 0
인공지능 바이러스 백신 SW	25	25 / 0
총 합	62	62 / 0

◦ 기능시험 평가점검표 #붙임 2 참조

2 - 1

○ 軍 환경 AI백신 Agent 호환성 검증 : 호환성 이상 및 오류 미식별

○ 보완/발전사항

구 분	의 견	보완 계획
1단계 기능시험	• AI정지를 관련 모델링 등 정지를 제작 평가항목이 제외되어 향후 軍 작전운영상 확인이 제한 • 軍 사령부 설치 서버는 실증평가를 위한 필수 소규모 구성으로 AI 정지를 제작 제한	AI 정지를 제작 중 소개교육 건의
	• 現 기술단계를 고려한 기능시험으로 백신 인터페이스 등이 미구현되어 운영상(안목도) 판단이 제한	
	• AI엔진, 클라우드 엔진 등 다중 검사로 다수 PC대상 에이전시 AI 서버, PC 부하 발생 예상	2단계 실증시 (서버/PC 성능측정, 악성코드 탐지율 등)
Agent 설치 및 호환성 검증	• 기존 軍 정보보호 솔루션과의 호환성 충돌은 미식별되었으나, Agent 설치 후 사용자 편의성 저하 관련 다수 의견(cpu 부하, 네트워크 속도 제하 등)	
조기에 성능 추가 평가항목 건의	• 사령부 자체 제작 unknown 악성코드 탐지율 측정	
	• 장상모듈(비악성행위)에 대한 오인탐지 여부 성능측정	

□ 향후 추진

○ 1단계 실증평가 결과 보고(국방부) : ~ 8월 4주

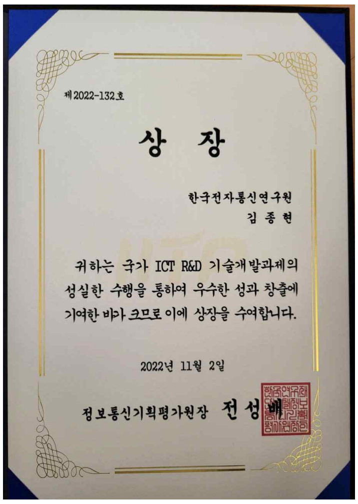
○ 2단계 실증평가(안) 협의(ETRI) 및 준비 : ~ 9월 1주

◦ 2단계 실증평가 : 9월 3주 ~ 4주(예정)

2 - 2

< 1단계 실증결과에 대한 국방부 공문(합격판정) >

○ 2022년도 ICT R&D 우수과제 및 **우수연구자(IITP 원장상) 수상**('22.11.02)



< 2022년도 IITP 주관 ICT R&D 우수과제 및 연구자 시상식 >

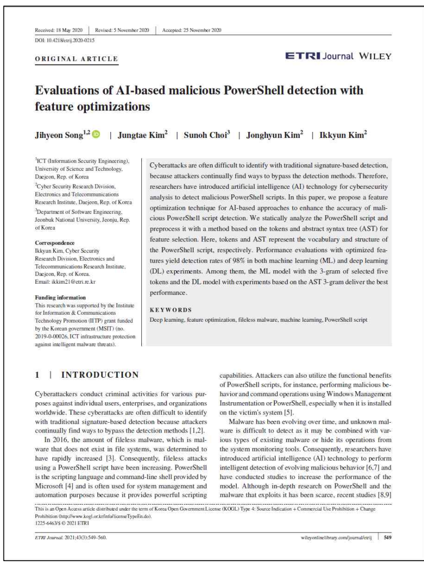
세계 최고 수준 대비 연구개발 수준

○ **(국내 최고)** 비실행형 악성코드 탐지 기술에 대한 **SCI 논문 게재 및 신뢰성 확보**

- 송지현 등, "Evaluations of AI-based Malicious PowerShell Detection with the Feature Optimizations," ETR Journal, Vol 43, No. 3, 2021년 6월
- 파워쉘 스크립트 토큰 단위 구문분석 및 토큰 조합 분석을 통한 특징인자 최적화 기술 개발 및 우수한 성능 확보(**탐지율: 96.97% / 오탐율: 0.5%**)

○ **(세계 최고)** 다양한 문서형(PDF, HWP) 악성코드 탐지를 위한 **바이트 스트림 기반 악성코드 탐지 기법 적용에 대한 우수성 확보** (IEEE Access, '22.05)

- 특징 추출 및 Byte Stream 기반 딥러닝탐지 모듈 (CNN) 연동 **(정확도 : 91.45%)**



Received: 18 May 2020 | Revised: 5 November 2020 | Accepted: 25 November 2020
DOI: 10.4218/etrij.2020-0215
ORIGINAL ARTICLE
ETRI Journal WILEY

Evaluations of AI-based malicious PowerShell detection with feature optimizations

Jihyeon Song[1,2] | Jungtae Kim[2] | Sunoh Choi[3] | Jonghyun Kim[2] | Ikkyun Kim[2]

[1]ICT (Information Security Engineering), University of Science and Technology, Daejeon, Rep. of Korea
[2]Cyber Security Research Division, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea
[3]Department of Software Engineering, Jeonbuk National University, Jeonju, Rep. of Korea

Correspondence
Ikkyun Kim, Cyber Security Research Division, Electronics and Telecommunications Research Institute, Daejeon, Rep. of Korea.
Email: ikkim21@etri.re.kr

Funding information
This research was supported by the Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korean government (MSIT) (no. 2019-0-00026, ICT infrastructure protection against intelligent malware threats).

Cyberattacks are often difficult to identify with traditional signature-based detection, because attackers continually find ways to bypass the detection methods. Therefore, researchers have introduced artificial intelligence (AI) technology for cybersecurity analysis to detect malicious PowerShell scripts. In this paper, we propose a feature optimization technique for AI-based approaches to enhance the accuracy of malicious PowerShell script detection. We statically analyze the PowerShell script and preprocess it with a method based on the tokens and abstract syntax tree (AST) for feature selection. Here, tokens and AST represent the vocabulary and structure of the PowerShell script, respectively. Performance evaluations with optimized features yield detection rates of 98% in both machine learning (ML) and deep learning (DL) experiments. Among them, the ML model with the 3-gram of selected five tokens and the DL model with experiments based on the AST 3-gram deliver the best performance.

KEYWORDS
Deep learning, feature optimization, fileless malware, machine learning, PowerShell script

1 | INTRODUCTION

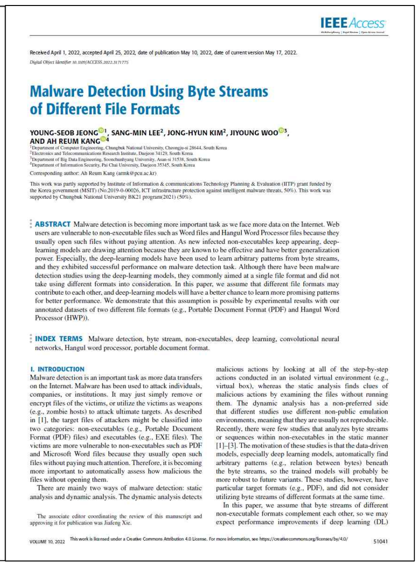
Cyberattackers conduct criminal activities for various purposes against individual users, enterprises, and organizations worldwide. These cyberattacks are often difficult to identify with traditional signature-based detection because attackers continually find ways to bypass the detection methods [1,2].

In 2016, the amount of fileless malware, which is malware that does not exist in file systems, was determined to have rapidly increased [3]. Consequently, fileless attacks using a PowerShell script have been increasing. PowerShell is the scripting language and command-line shell provided by Microsoft [4] and is often used for system management and automation purposes because it provides powerful scripting capabilities. Attackers can also utilize the functional benefits of PowerShell scripts, for instance, performing malicious behavior and command operations using Windows Management Instrumentation or PowerShell, especially when it is installed on the victim's system [5].

Malware has been evolving over time, and unknown malware is difficult to detect as it may be combined with various types of existing malware or hide its operations from the system monitoring tools. Consequently, researchers have introduced artificial intelligence (AI) technology to perform intelligent detection of evolving malicious behavior [6,7] and have conducted studies to increase the performance of the model. Although in-depth research on PowerShell and the malware that exploits it has been scarce, recent studies [8,9]

This is an Open Access article distributed under the term of Korea Open Government License (KOGL) Type 4: Source Indication + Commercial Use Prohibition + Change Prohibition (http://www.kogl.or.kr/info/licenseTypeEn.do).
1225-6463/$ © 2021 ETRI

ETRI Journal. 2021;43(3):549–560. wileyonlinelibrary.com/journal/etrij | 549



IEEE Access
Received April 1, 2022, accepted April 25, 2022, date of publication May 10, 2022, date of current version May 17, 2022.
Digital Object Identifier 10.1109/ACCESS.2022.3171775

Malware Detection Using Byte Streams of Different File Formats

YOUNG-SEOB JEONG[1], SANG-MIN LEE[2], JONG-HYUN KIM[2], JIYOUNG WOO[3], AND AH REUM KANG[4]
[1]Department of Computer Engineering, Chungbuk National University, Cheongju-si 28644, South Korea
[2]Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea
[3]Department of Big Data Engineering, Soonchunhyang University, Asan-si 31538, South Korea
[4]Department of Information Security, Pai Chai University, Daejeon 35345, South Korea
Corresponding author: Ah Reum Kang (armk@pcu.ac.kr)

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2019-0-00026, ICT infrastructure protection against intelligent malware threats, 50%). This work was supported by Chungbuk National University BK21 program(2021) (50%).

ABSTRACT Malware detection is becoming more important task as we face more data on the Internet. Web users are vulnerable to non-executable files such as Word files and Hangul Word Processor files because they usually open such files without paying attention. As new infected non-executables keep appearing, deep-learning models are drawing attention because they are known to be effective and have better generalization power. Especially, the deep-learning models have been used to learn arbitrary patterns from byte streams, and they exhibited successful performance on malware detection task. Although there have been malware detection studies using the deep-learning models, they commonly aimed at a single file format and did not take using different formats into consideration. In this paper, we assume that different file formats may contribute to each other, and deep-learning models will have a better chance to learn more promising patterns for better performance. We demonstrate that this assumption is possible by experimental results with our annotated datasets of two different file formats (e.g., Portable Document Format (PDF) and Hangul Word Processor (HWP)).

INDEX TERMS Malware detection, byte stream, non-executables, deep learning, convolutional neural networks, Hangul word processor, portable document format.

I. INTRODUCTION

Malware detection is an important task as more data transfers on the Internet. Malware has been used to attack individuals, companies, or institutions. It may just simply remove or encrypt files of the victims, or utilize the victims as weapons (e.g., zombie hosts) to attack ultimate targets. As described in [1], the target files of attackers might be classified into two categories: non-executables (e.g., Portable Document Format (PDF) files) and executables (e.g., EXE files). The victims are more vulnerable to non-executables such as PDF and Microsoft Word files because they usually open such files without paying much attention. Therefore, it is becoming more important to automatically assess how malicious the files without opening them.

There are mainly two ways of malware detection: static analysis and dynamic analysis. The dynamic analysis detects malicious actions by looking at all of the step-by-step actions conducted in an isolated virtual environment (e.g., virtual box), whereas the static analysis finds clues of malicious actions by examining the files without running them. The dynamic analysis has a non-preferred side that different studies use different non-public emulation environments, meaning that they are usually not reproducible. Recently, there were few studies that analyzes byte streams or sequences within non-executables in the static manner [1]–[3]. The motivation of these studies is that the data-driven models, especially deep learning models, automatically find arbitrary patterns (e.g., relation between bytes) beneath the byte streams, so the trained models will probably be more robust to future variants. These studies, however, have particular target formats (e.g., PDF), and did not consider utilizing byte streams of different formats at the same time.

In this paper, we assume that byte streams of different non-executable formats complement each other, so we may expect performance improvements if deep learning (DL)

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.
VOLUME 10, 2022

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

51041

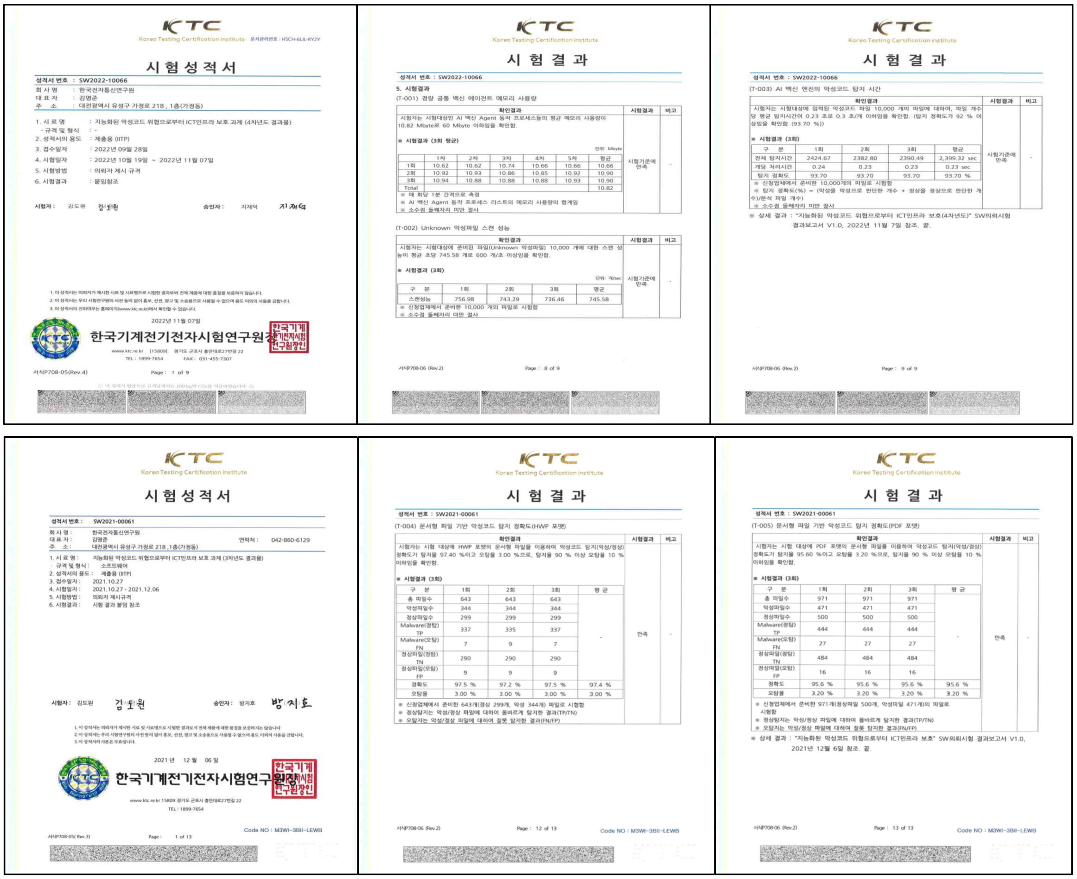
< SCI급 논문 IEEE Access, Vol 10, No. 3, IF 3.476 >

기술수준 공인 성과

○ **(실효성 검증)** 국방실증 1/2단계 평가 항목 전체에 대하여 "기준 충족"으로 평가되었으며, 기능/성능 시험 시 국방부의 별도 요구사항에 대해서도 시험을 진행함으로써, 해당 기술의 **국방 인공지능 백신체계 구축을 위한 핵심 원천기술 확보**

○ **(공인시험 검증)** 국제공인시험인증기관인 한국기계전기전자시험연구원 (KTC)을 통해서 **정량적 성능목표에 대한 공인시험 검증 완료 (기존 상용 백신 에이전트 대비 월등한 성능 확보)**

- 경량 공통 백신 에이전트 메모리 사용량: **10.82 Mbyte**
- Unknown 악성파일 스캔 성능: **745건/초**
- AI 백신 엔진의 악성코드 탐지 시간: **평균 0.23초**
- 문서형 파일(HWP, PDF) 기반 악성코드 탐지 정확도: 탐지율/오탐율 **97.4%/3.0%** (HWP), **95.6%/3.2%**(PDF)



< 공인시험인증기관(KTC)의 정량적 성능시험 결과 >

○ **(학술적 검증)** 비실행형 및 문서형 악성코드 탐지 기술 등에 대한 SCI 저널 7건 게재를 통한 신뢰성 확보

- 악성 파워셸 (PowerShell) 탐지를 위한 특성인자 전처리 기능 설계 및 딥러닝 모델 최적화 적용(**탐지율: 96.97%/오탐율: 0.5% 확보**)

4. 성과의 활용도 및 파급효과

경제 활성화 효과

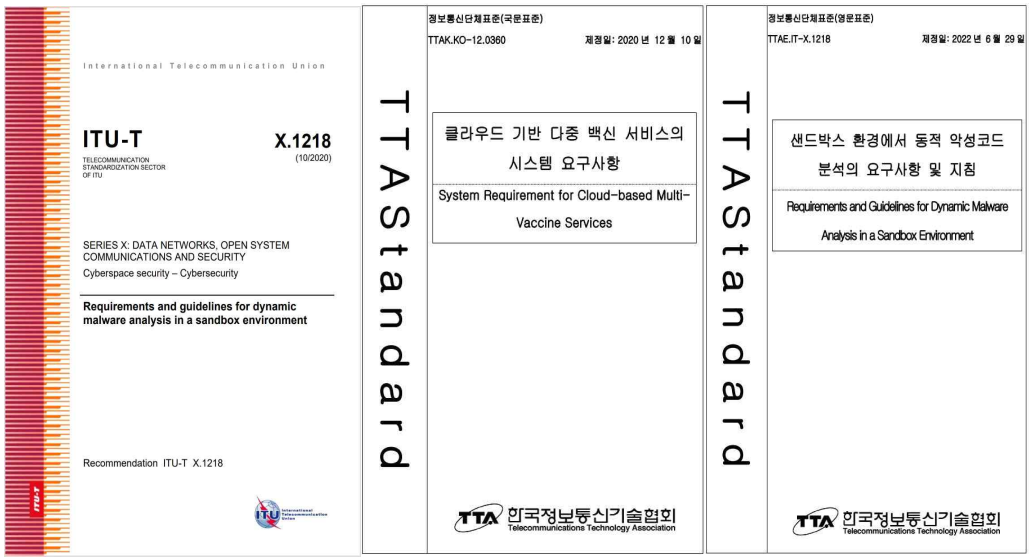
기업 경쟁력 향상

○ 국내 백신사와의 협업을 통한 클라우드 기반 다중 AI백신 시스템 개발 및 국방망 실증을 통해서 해당 평가 전체에 대하여 “기준 충족”의 결과를 도출함으로써, **국방 인공지능 백신체계의 원천기술 확보 및 향후 구축 사업을 위한 경쟁력 확보**

○ 다중 분석 플랫폼 기술을 활용하여 기존 기술의 대체 및 새로운 악성코드 탐지 시장 확보를 통한 **상용시제품 개발 및 기술 사업화 실적**(126.39백만원) **달성**

< 다중 악성코드 분석플랫폼(상용시제품) 소개 브로셔 >

○ 클라우드 다중 AI 백신 기술에 대한 **국제표준 1건**(ITU-T X.1218) 및 **국내표준 3건**(TTA 단체표준) **제정**을 통한 **국내 기술의 글로벌 경쟁력 확보**



< ITU-T SG17 국제표준 및 TTA PG503 국내표준 >

산업 경쟁력 향상

○ 정보보호 산업의 초석인 안티바이러스 산업의 부흥에 따른 우수 인재를 발굴·흡수함으로써 산업 경쟁력 강화

○ 보안 사각지대에 놓인 벤처/중소기업을 대상으로 신종 악성코드 공격 대응 서비스 제공 및 새로운 백신기술의 보급 가속화 실현

○ 클라우드 기반 다중 AI 백신 기술을 통하여 신·변종 악성코드에 대한 신속한 대응과 분석가의 분석 시간을 최소화할 수 있음

경제적 파급효과

○ (파급효과 전망)

- AI 기반 악성코드 분석 기술을 통해 침해사고 대응력을 강화함으로써 사회적·국가적 피해를 최소화할 수 있음
- 클라우드 기반 AI 악성코드 분석플랫폼을 개발/보급하여 개별 기업의 중복 투자로 인한 물적/인적/시간 관련 비용 절감 (민간 실증서비스를 통한 유효성 검증)

국가·사회적 파급효과

○ 해결해야 할 국가·사회문제

- 인공지능 백신 체계의 구축 및 확산을 위한 방안을 제시함으로써 최근 국방망에서 발생한 공급망 공격에 대하여 신속한 대응 가능
- 클라우드 환경의 AI 기반 악성코드 분석 기술 개발을 통해 사이버 테러 및 사이버 전에 대한 예방 능력 제고 및 신속한 대응력 확보 (국방 인공지능 백신체계 적용)

○ 성과에서 개발된 기술적 솔루션

- AI 기술을 활용한 악성코드 분석 및 대응은 기존 방식의 한계점을 넘어, 능동적으로 악성코드를 학습함으로써 알려지지 않은 잠재적 위협에 대한 대응이 가능
- 최근 클라우드 환경이 널리 보급·발전함에 따라 다양한 AI 기반 악성코드 분석 엔진을 탑재하여 운영함으로써 지능화된 악성코드 공격에 대한 효과적인 대응이 가능

○ 국가·사회적 파급효과

- 알려지지 않은 악성코드에 효과적인 탐지·대응 가능, 기존 백신 솔루션의 한계점 극복 효과 기대
- AI 기반 악성코드 분석 기술 개발을 통해 신·변종 공격을 탐지, 정밀분석, 침해 시도 추이분석 등의 사이버 침해 대응체계 고도화 기대

부록 정량적 연구 성과

[기술적 성과]

□ 지식재산권(특허, 실용신안, 의장, 디자인, 상표, 규격, 신품종, 프로그램)

- 국제 등록

번호	지식재산권 등 명칭 (건별 각각 기재)	국명	출원		등록		기여율
			출원일	출원번호	등록일	등록번호	
1	Apparatus for selecting representative token from detection names of multiple vaccines, method therefor, and computer readable recording medium storing program for performing the method	미국	‘21.05.25	17/329,769	‘22.01.25.	US 11,232,200B2	100
2	PACKER CLASSIFICATION APPARATUS AND METHOD USING PE SECTION INFORMATIONS	미국	‘20.05.29	16/887,436	‘22.08.30.	US 11,429,819B2	100

- 국제 출원

번호	지식재산권 등 명칭 (건별 각각 기재)	국명	출원		등록		기여율
			출원일	출원번호	등록일	등록번호	
1	PE 섹션 정보를 이용한 패커 유형 분류 장치 및 방법	미국	‘20.05.29	16/887,436			100
2	악성 스크립트 탐지 장치 및 방법	미국	‘20.11.20	17/100,541			100
3	다중백신의 탐지명으로부터 대표토큰을 선정하기 위한 장치, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	미국	‘21.05.25	17/329,769			100
4	DGA 생성도메인 탐지 및 분류 방법	미국	‘21.08.04	17/393,567			100
5	가변 길이 명령코드를 이용한 알려지지 않은 악성코드 탐지 장치 및 이를 이용한 방법	미국	‘21.08.30	17/461,337			100

- 국내 등록

번호	지식재산권 등 명칭 (건별 각각 기재)	국명	출원		등록		기여율
			출원일	출원번호	등록일	등록번호	
1	다중 백신의 탐지명으로부터 대표 토큰을 선정하기 위한 장치, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	대한민국	‘20.06.26.	10-2020-0078570	‘20.12.31	10-2199704	100
2	PE 섹션 정보를 이용한 패커 유형 분류 장치 및 방법	대한민국	‘19.07.25	10-2019-0090031	‘21.01.08.	10-2202911	100
3	관제 대응을 위한 통합진단정보를 제공하기 위한 장치, 이를 위한 방법 및 이 방법을 실행시키기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	대한민국	‘20.06.26	10-2020-0078563	‘21.5.27	10-2259884	100
4	악성코드 진단시스템 및 진단방법	대한민국	‘20.11.16.	10-2020-0152827	‘22.07.25	10-2426504	100
5	DGA 생성도메인 탐지 및 분류 방법	대한민국	‘20.12.01	10-2020-0165503	‘23.01. (예정)		100

- 국내 출원

번호	지식재산권 등 명칭 (건별 각각 기재)	국명	출원		등록		기여율
			출원일	출원번호	등록일	등록번호	
1	PE 섹션 정보를 이용한 패커 유형 분류 장치 및 방법	대한민국	'19.07.25	10-2019-0090031	'21.01.08.	10-2202911	100
2	악성 스크립트 탐지 장치 및 방법	대한민국	'20.02.05.	10-2020-0013795			100
3	관제 대응을 위한 통합진단정보를 제공하기 위한 장치, 이를 위한 방법 및 이 방법을 실행시키기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	대한민국	'20.06.26	10-2020-0078563	'21.5.27	10-2259884	100
4	다중 백신의 탐지명으로부터 대표 토큰을 선정하기 위한 장치, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	대한민국	'20.06.26	10-2020-0078570	'20.12.31	10-2199704	100
5	대규모 범주형 데이터 처리 장치 및 방법	대한민국	'20.07.30.	10-2020-0095391			100
6	가변 길이 명령코드를 이용한 알려지지 않은 악성코드 탐지 장치 및 이를 이용한 방법	대한민국	'21.05.11	10-2021-0060608			100
7	악성코드 진단시스템 및 진단방법	대한민국	'20.11.16.	10-2020-0152827			100
8	DGA 생성도메인 탐지 및 분류 방법	대한민국	'20.12.01	10-2020-0165503			100
9	효율적인 악성 위협 탐지를 위한 valuable alert 선별 방법	대한민국	'21.11.23	10-2021-0162305			100
10	어셈블리 언어 모델 기반 악성코드 탐지 방법 및 장치	대한민국	'22.05.17	10-2022-0059945			100
11	악성코드 탐지 방법 및 장치	대한민국	'22.07.05	10-2022-0082551			100
12	가상 머신 스케일링을 이용한 인터넷 기반 악성 코드 탐지 엔진 업데이트 장치 및 방법	대한민국	'22.09.28	10-2022-0123255			100
13	악성코드 변종 분석을 위한 AI 모델의 견고성 측정 시스템 및 어플리케이션	대한민국	'22.09.19	10-2022-0117936			100

□ 저작권(소프트웨어, 서적 등)

번호	저작권명	등록일	등록번호	기여율
1	PE(Portable Executable) 파일기반 Feature(특성 인자) 추출 소프트웨어	'19.12.10	C-2019-036918	100
2	헥사 명령코드 기반 실행파일 전처리 및 딥러닝 학습테스트	'20.11.19	C-2020-043609	100
3	PE(Portable Executable) 파일을 이용한 LightGBM 기반 악성코드 탐지 소프트웨어	'20.12.07	C-2020-048198	100
4	바이로봇 AI 백신 에이전트 0.5	'20.11.27.	C-2020-043939	100
5	악성코드 통합 탐지명을 서비스하기위한 API 시스템	'21.05.12	C-2021-020130	100
6	악성코드 통합 탐지명 분석결과를 모니터링하는 프론트엔드 시스템	'21.05.12	C-2021-020131	100
7	악성코드 통합 탐지명 추출 엔진 프로그램	'21.05.12	C-2021-020132	100
8	PE(Portable Executable) 파일을 이용한 YARA rule(야라 룰) 기반 indicator feature(인디케이터 피처) 추출 기술	'21.12.01	C-2021-052133	100
9	PE(Portable Executable) 파일을 이용한 앙상블 알고리즘 기반 악성코드 탐지 기술	'21.12.01	C-2021-052134	100
10	바이로봇 AI 백신 에이전트 0.9	'21.12.09	C-2021-054097	100
11	리눅스용 바이로봇 AI 백신 에이전트 0.1	'21.12.09	C-2021-054098	100
13	인공지능 백신 시각화 프로그램	'21.12.21	C-2021-056783	100
14	언어모델 기반 악성코드 정적 분석 프로그램	'21.12.21	C-2021-056790	100

□ 표준화

번호	수행 기관명	표준화 주제	표준화 기구	표준화 단계	관련 번호	제출(채택)일	국가
1	ETRI	Proposal for a revised text for draft Recommendation X.rdmase: Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment	ITU-T	기고서 제출	C 728	2019.08.19	스위스
2	ETRI	Revised draft text for X.rdmase: Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment	ITU-T	기고서 채택	TD2362	2019.09.03	스위스
3	ETRI	다중 백신 서비스 환경에서 STIX 기반의 악성코드 분석 정보 교환 포맷	TTA	기고서 제출	2019-1328	2019.11.22	대한민국
4	ETRI	Revised baseline text for X.rdmase: Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment	ITU-T SG17	기고서 제출	C 813	2020.02.17	스위스
5	ETRI	Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment	ITU-T SG17	기고서 채택	TD2858	2020.03.23	스위스
6	ETRI	Requirements and guidelines for dynamic malware analysis in a sandbox environment	ITU-T SG17	표준안 채택	X.1218	2020.10.29	스위스
7	ETRI	인텔리전스 정보의 신뢰 및 자동화된 교환(TAXII) 버전 2.1	TTA PG503	기고서 제출	2020-P0697	2020.09.21.	대한민국
8	ETRI	인텔리전스 정보의 신뢰 및 자동화된 교환(TAXII) 버전 2.1	TTA PG503	기고서 채택	2020-0710	2020.11.13.	대한민국
9	ETRI	클라우드 기반 다중 백신 서비스의 시스템 요구사항	TTA PG503	표준안 채택	TTAK.KO-12.0360	2020.11.25.	대한민국
10	ETRI	샌드박스 환경에서 동적 악성코드 분석의 요구사항 및 지침	TTA PG503	기고서 제출	2021-P1836	2021.07.30	대한민국
11	ETRI	샌드박스 환경에서 동적 악성코드 분석의 요구사항 및 지침	TTA PG503	기고서 채택	2021-2131	2021.09.01	대한민국
12	ETRI	인텔리전스 정보의 신뢰 및 자동화된 교환(TAXII) 버전 2.1	TTA PG503	표준안 채택	TTAE.OT-12.0022	2021.12.08	대한민국
13	ETRI	Proposal for new work item: Security requirements and countermeasures for targeted email attacks	ITU-T SG17	기고서 제출	C 21	2022.05.09	스위스
14	ETRI	1st Revised baseline text for X.sr-ctea: Security requirements and countermeasures for targeted email attacks	ITU-T SG17	기고서 제출	C 149R3	2022.08.10	스위스
15	ETRI	Security requirements and countermeasures for targeted email attacks	ITU-T SG17	기고서 채택	TD244	2022.05.18	스위스
16	ETRI	X.sr-ctea, Security requirements and countermeasures for targeted email attacks	ITU-T SG17	기고서 채택	TD561	2022.09.02	스위스
17	ETRI	샌드박스 환경에서 동적 악성코드 분석의 요구사항 및 지침	TTA PG503	표준안 채택	TTAE.IT-X.1218	2022.06.29	대한민국

[과학적 성과]

□ 국내 및 국외 논문 게재

번호	논문명	학술지명	호	국명	발행기관	SCI 여부 (SCI/비SCI)	게재일	등록번호
1	Anomaly Based Unknown Intrusion Detection in Endpoint Environments	Electronics	6	스위스	MDPI	SCI(E)	’20.06	2079-9292
2	Malware Detection of Hangul Word Processor Files Using Spatial Pyramid Average Pooling	Sensors	20	스위스	MDPI	SCI(E)	’20.09	1424-8220
3	Evaluations of AI-based Malicious PowerShell Detection with the Feature Optimizations	ETRI Journal	43/3	대한민국	ETRI	SCI(E)	’21.06	1225-6463
4	Cost-effective valuable data detection based on the reliability of artificial intelligence	IEEE Access	9	미국	IEEE	SCI(E)	`21.07	2169-3536
5	정보보호 분야의 XAI 기술 동향	정보보호학회지	31/5	대한민국	한국정보보호학회	비SCI	’21.10	1598-3978
6	AI백신체계 연구개발 제품의 국방분야 실증 프로세스 개선 연구	융합보안논문지	21/4	대한민국	한국융합보안학회	비SCI	’21.10	2508-7460
7	Android malware dataset construction methodology to minimize bias–variance? tradeoff	ICT Express	On-Line	네덜란드	Elsevier	SCI	’21.12	2405-9595
8	Unknown 악성코드 분석을 위한 AI 기반 시각화 플랫폼 (기여율 50%)	국방과 보안	6	대한민국	국방보안연구소	비SCI	’21.12	2671-8111
9	Malware Detection Using Byte Streams of Different File Format (기여율 50%)	IEEE Access	Vol. 10	미국	IEEE	SCI	’22.05.	2169-3536
10	Automatic False Alarm Detection Based on XAI and Reliability Analysis	MDPI Applied Sciences	Vol. 12	스위스	MDPI	SCI	’22.07	2076-3417

□ 국내 및 국제학술회의 발표

번호	발표 제목	회의명칭	발표일	장소	국명
1	Android Malware Similarity Clustering using Method based Opcode Sequence and Jaccard Index	ICTC 2019	2019.10	제주	대한민국
2	High-Speed Search Technology based on Ssdeep	ICONI 2019	2019.12		베트남
3	dhash feature를 활용한 머신러닝 기반 리눅스 악성코드 분석기술 연구	한국정보보호학회 하계학술대회 논문집	2019.06	부산	대한민국
4	TF-IDF 기반 PE파일 Embedding 기법을 통한 악성코드 유형분류 기술 연구	한국정보보호학회 하계학술대회 논문집	2019.06	부산	대한민국
5	Smart Building에서 운영 가능한 DLL Injection 기반 경량 암호기술에 관한 연구	한국정보보호학회 하계학술대회 논문집	2019.06	부산	대한민국
6	A Study on Detecting Suspicious and Malicious Activity based on AutoEncoder	APIC-IST 2020	2020.7	서울	대한민국
7	Malware Family Classification Model using Xception Network	SMA 2020	2020.9	제주	대한민국
8	Sumav: A Scheme for Selecting a Keyword from Detection Names using Conditional Probability	ICTC 2020	2020.10	제주	대한민국
9	Malware Response Naming Scheme for Security Control Service	ICTC 2020	2020.10	제주	대한민국
10	Design of Integrated Messenger Anti-virus System using Chatbot Service	ICTC 2020	2020.10	제주	대한민국
11	Evaluation of Image Similarity Algorithms for Malware Fake-Icon Detection	ICTC 2020	2020.10	제주	대한민국
12	Entry Point를 활용한 머신러닝 기반 악성코드 분석 연구	한국정보보호학회 하계학술대회 논문집	2020.7	온라인	대한민국
13	LightGBM을 이용한 IDS 웹 이벤트 로그 분류 기법	한국정보통신학회 춘계종합학술대회 논문집	2020.7	온라인	대한민국

14	LOF 기반 공격 의심 행위 탐지기술 연구	한국정보통신학회 춘계종합학술대회 논문집	2020.7	온라인	대한민국
15	Research on Autoencdoer Technology for Malware Feature Purification	SNPD 2021	2021.1	온라인	베트남
16	LIME 기반 악성코드 그룹분류 결과 해석	한국정보보호학회 하계학술대회 논문집	2021.6	온라인	대한민국
17	개선된 데이터 마이닝 기법을 이용한 악성코드 탐지 연구 동향	한국통신학회 하계학술대회 논문집	2021.6	온라인	대한민국
18	A study on the Interpretability of Malware Detection based on Artificial Intelligence	WISA 2021	2021.8	제주	대한민국
19	Research on improvement of anomaly detection performance in industrial control systems	WISA 2021	2021.8	제주	대한민국
20	Netflow를 이용한 이상 공격징후 탐지방안 연구	한국정보보호학회 충청지부 학술대회 논문집	2021.8	온라인	대한민국
21	인공지능 기반 악성코드 분석에서의 모델 편향완화 방안 연구	한국통신학회 동계종합학술발표회	2022.02	온라인	대한민국
22	자동화된 Data Cleaning 기반 AI 성능 향상 방안 연구	한국정보보호학회 하계학술대회 논문집	2022.06	부산	대한민국

[경제적 성과]

□ 기술 거래(이전) 등

번호	기술 이전 유형	기술 실시 계약명	기술 실시 대상 기관	기술 실시 발생일	기술료 (해당 연도 발생액)	누적 징수 현황
1	기술이전 (정액기술료)	Hex-Opcode를 이용한 AI기반 PE 악성코드 분석 기술	㈜젠토	'20.12.10	27,500,000 원	27,500,000 원
2	기술이전 (정액기술료)	언어모델 기반 악성코드 정적 분석 기술	쿤텍 주식회사	'21.12.13	38,500,000 원	38,500,000 원
3	기술이전 (정액기술료)	AI기반 PE 악성코드 분석 및 시각화 도구 기술	㈜젠토	'21.12.13	11,000,000 원	11,000,000 원

□ 사업화 현황

(단위: 명, 년)

번호	사업화 방식	사업화 형태	지역	사업화명	내용	업체명	매출액		매출 발생 연도	기술 수명
							국내	국외		
1	자가실시	신제품 개발	국내	악성코드 및 비정상 트래픽 대응시스템 재구축 사업	시제품 납품	이스트 시큐리티 (NH농협은행)	30,800천원	-	2020	
2	자가 실시	기존 제품 개선	국내	악성코드 및 위협 정보 대응 Feed-Service 사업	ESTsecurity Threat Inside (MIST API)	한국인터넷 진흥원	44,000천원		2021	
3	자가 실시	기존 제품 개선	국내	악성코드 및 위협 정보 대응 Feed-Service 사업	ESTsecurity Threat Inside (MIST API)	엠퍼시스 정보기술	51,590천원		2021	