

캡스톤 디자인 2024-1 최종 발표

# PLATFORM GIPS

생성형 침입방지 기술 기반 보안 플랫폼

---

| 국민대학교 정보보호연구실 & (주)누리랩 | 산학협력 34조 |  
| 지도교수 윤명근 | 엄석현 김태경 김태윤 박준서 |



nurilab

CONTENTS

# 목차

- 프로젝트 배경
- 프로젝트 목표
- 기술 및 기능 소개
- 결론

PLATFORM GIPS

생성형 침입방지 기술 기반 보안 플랫폼

01

## 생성형 AI으로 인한 악성코드 폭발적 증가

- 공격자들의 생성형AI (WormGPT 등) 악용
- 변종 악성코드 대량 생산 및 유포 건수 증가

02

## 악성코드 대응을 위한 보안인력 부족

- 악성코드 발생 수는 하루 40~50만개
- 악성코드 발생 수 대비 보안인력 절대적 부족

03

## 사용자에게 설명 가능한 탐지방법 필요성 증대

- 악성코드를 판단한 기준 설명 필요성 증대
- 사용자에게 정확한 정보제공 필요

## 생성형 침입방지 기술기반 보안 플랫폼 PLATFORM GIPS



01

### 탐지 규칙 생성 및 적용

- 파일로부터 공통 시그니처 추출 후 탐지 규칙 생성
- 생성된 탐지 규칙을 적용하여 악성 파일 탐지

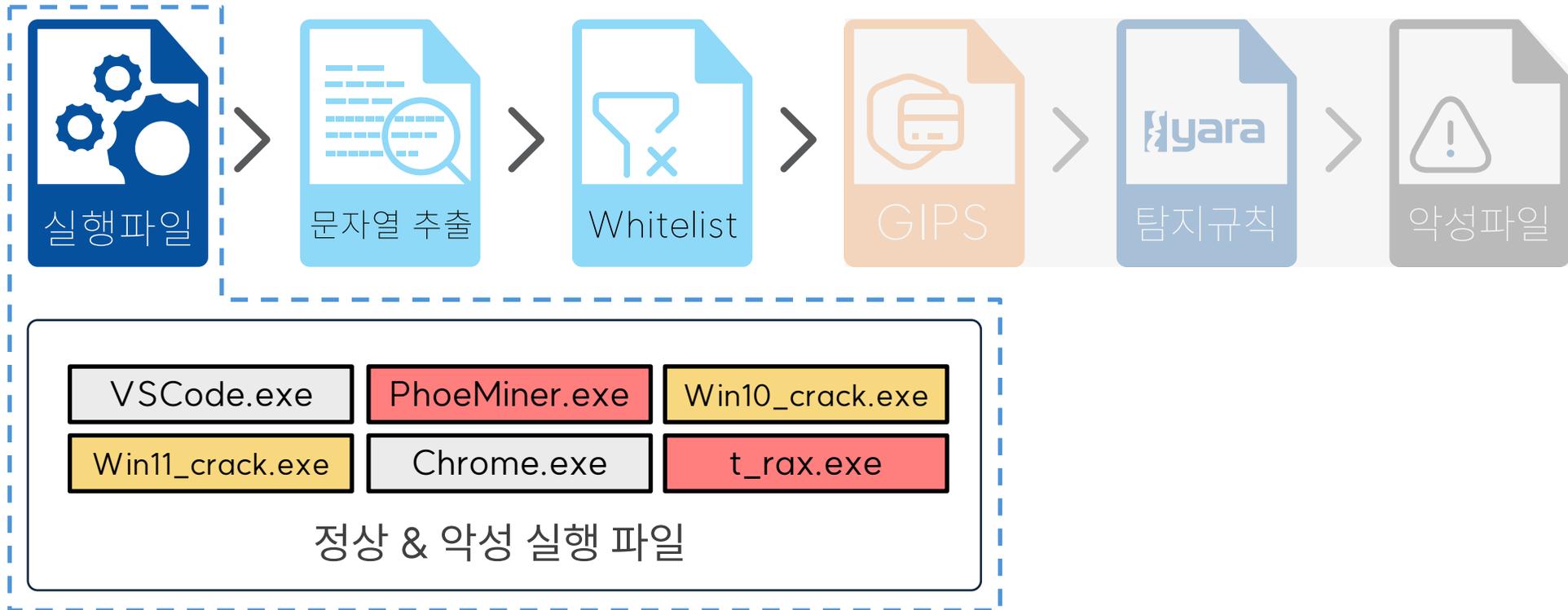
02

### 공격 시각화

- 다양한 기법으로 플랫폼에서 탐지한 공격을 시각화
- 보안 전문가가 위협을 시각적으로 파악 가능

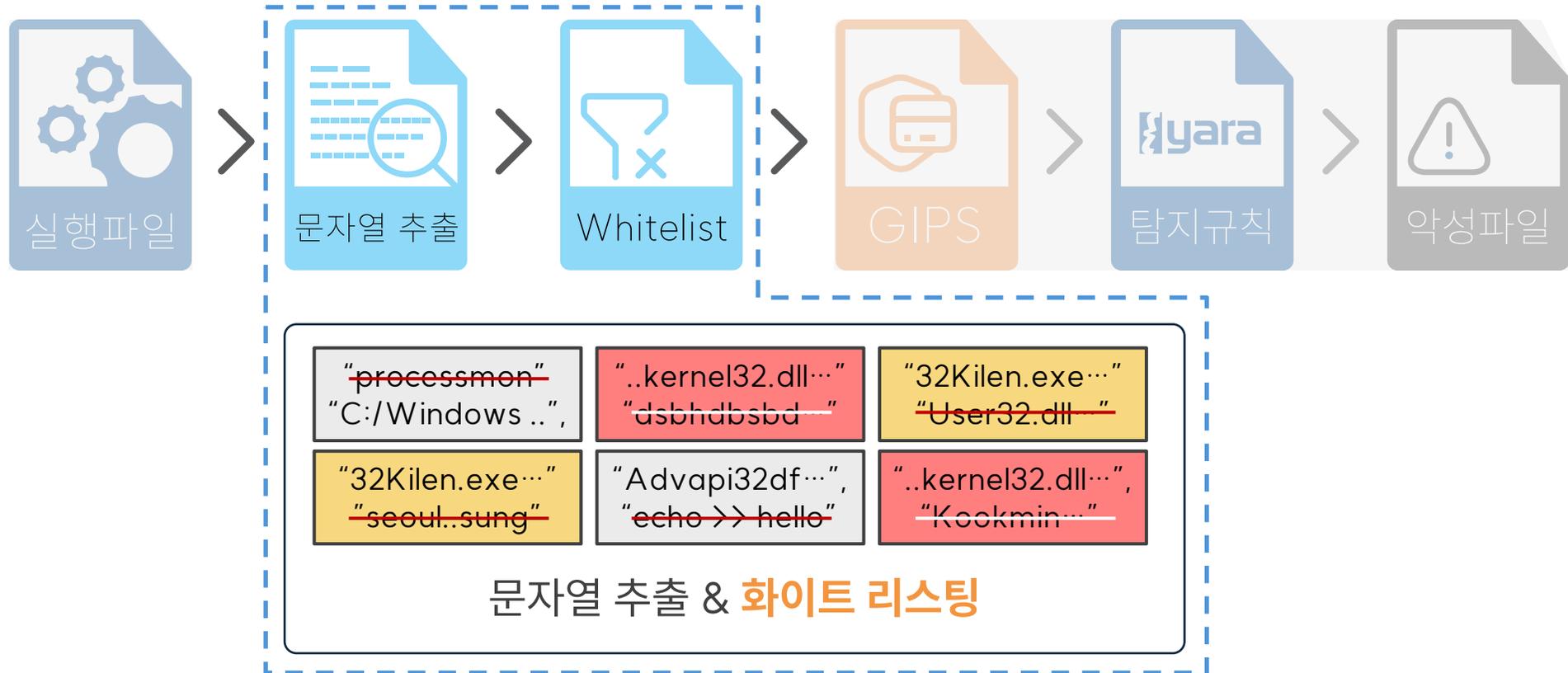
## 01

### 실행 파일 업로드



## 02

### 데이터 전처리



03

**생성형 침입 방지 기술(GIPS\*: Generative Intrusion Prevention on data Stream)**을 사용해  
유의미한 시그니처가 나올 수 있는 **그룹을 식별**하고 이를 이용해 **시그니처를 추출**



\* HyungBin Seo, and MyungKeun Yoon. "Generative intrusion detection and prevention on data stream." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023.

**Platform GIPS**  
생성형 침입방지 보안 플랫폼

☰ 대시보드

📄 탐지규칙 생성

- Yara Rule 수동생성
- Yara Rule 자동생성
- Yara Rule DB관리

📄 탐지규칙 적용

- Yara Rule 적용

📄 정적파일 분석

- 단일 PE 파일 분석

📄 탐지통계 조회

- 통계 시각화

Dashboard

## 대시보드

주간 유입량 <sup>?</sup>  
**2,540** ↗ 12.5%

일일 유입량  
**1,376** ↘ 1.7%

탐지 시그니처 개수  
**12,597**

**탐지 파일 종류**  
탐지한 파일 유형을 확인해보세요.

**탐지 주요 시그니처**  
스트림에서 추출한 시그니처를 확인해보세요.

**Platform GIPS**  
상성형 점입방지 보안 플랫폼

- ☰ 대시보드
- 📄 탐지규칙 생성
  - Yara Rule 수동생성
  - Yara Rule 자동생성
  - Yara Rule DB관리
- 📄 탐지규칙 적용
  - Yara Rule 적용
- 📄 정적파일 분석
  - 단일 PE 파일 분석
- 📄 탐지통계 조회
  - 통계 시각화

Dashboard
2024-05-21 PM 11:23:40

## 대시보드

주간 유입량 ↗ 12.5%

**2,540**

일일 유입량 ↘ 1.7%

**1,376**

탐지 시그니처 개수

**12,597**

악성 분류건수 ↻

**92,913**

**탐지 파일 종류**  
어떤 파일을 탐지했는지 확인해보세요.

종류	비율
exe	59.9%
lib	22.9%
sys	10.4%
obj	6.7%

**탐지 주요 시그니처**  
스트림에서 추출한 시그니처를 확인해보세요.

**개별파일 검사결과**  
개별파일 검사결과를 확인해보세요.

📄 내보내기

번호	일시	파일명	탐지결과	탐지 개수
1	2024-05-17 16:06:34	cnn.exe	● 정상	0
2	2024-05-17 16:06:50	index.exe	● 공격	1
3	2024-05-17 16:07:01	kma.exe	● 정상	0
4	2024-05-20 16:55:17	KLT2000.dll	● 공격	258

## 플랫폼 주요정보를 한눈에 확인 할 수 있도록 대시보드 형태의 메인 화면 구성

- 카드 UI 형태로 보기 쉽게 구성
- 기본적인 통계 정보 시각화
- 개별 파일 검사 결과 정보 확인 가능



```
rule yara : banker
{
  meta:
    description = "This is just an example"
    in_the_wild = true

  strings:
    $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
    $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
    $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

  condition:
    $a or $b or $c
}
```

프로젝트 사용 조건

String 시그니처  
생성후 사용



**YARA RULE?** 악성코드 시그니처를 이용해서 악성 코드의 종류를 식별하고 분류하는 목적으로 사용되는 규칙

- VirusTotal사 개발 & 보안분야에서 널리 사용되는 규칙
- 오픈 소스 & 멀티 플랫폼 지원 [Windows, Linux, Mac]

Auto Generate Yara Rule

## Yara Rule 자동 생성

분석을 원하는 파일을 끌어오거나 [클릭](#)해 업로드해주세요.

51개

- b3de05b73e2f53ea18a5c4a5f6c28fb0 [0.22MB] × 삭제
- b3dedfa844e7f6f13672fca0911e309 [0.3MB] × 삭제
- b3e5f6692b1e6d74be822acbb05aa550 [0.25MB] × 삭제
- b3e6cc96978d0e825331f75addd77e80 [0MB] × 삭제
- b3e8e8b1063e0b6257156dd90edbba50 [1.13MB] × 삭제

분석하기

01 탐지 규칙 자동 생성을 위한 파일 업로드



Auto Generate Yara Rule

## Yara Rule 자동 생성

↶ 다른 파일로 생성하기

### 추출 시그니처

&:at\*f 545@5d5l5p5\5`5h5l5p5t5x5l5 ejsslmlmvv k\$wsac  
uqies a pc<k\$:q if2x&y 1m2a2w2 90:j:o c:}(te  
1@do/t 00,00,00,00 ecriycalse +eelaelaee btrrb  
ljeltjel meu+sqnx &sa2a'g \system32\netsetup.exe bnoon  
nov+wni <rb2#' v:|\@'d9} ppe19-' d!4lc\* hk1t+0  
/0l'\~kua \lotus\_workflow\_v7.0\_crack.exe z1qhg# \emule\_kad  
lpkunj ,,"i2k :+:h:o:n: 5/~%gk vel\nel !#lq#"ssry~  
iiiiimee) \adobe\_font\_folio\_crackandserial.exe \ad-aware.exe 1f  
\quake 3 - the arena no cd crack.exe ein]err[+ \*mo1:mc htiht\_-

02 자동 분석하여 시그니처 추출 및 탐지 규칙 생성

## 자동 생성 탐지 Yara Rule

Yar 파일 다운로드

```
1 import "pe"
2
3 rule test1
4 {
5     strings:
6         $sig1 = "&:at*f" nocase
7         $sig2 =
8             "545@5d5l5p5\5`5h5l5p5t5x5l5"
9             nocase
10        $sig3 = "ejsslmlmvv" nocase
11        $sig4 = "k$wsac" nocase
12        $sig5 = "6utm2}" nocase
13        $sig6 = "&g\"f e" nocase
14        $sig7 = "\\half-life 2 no cd crack.
15        exe" nocase
16        $sig8 = "898\\8|8" nocase
17        $sig9 = "\\sony_k700_dateimanager.
18        exe" nocase
19        $sig10 = "29ut+s" nocase
20        $sig11 = "inverflow4tc," nocase
21        $sig12 = "7#7<7\\7d7h7l7p7t7x7|7"
```

Manual Generate Yara Rule

### Yara Rule 수동 생성

Yara Rule 생성기

Yara Rule 이름

String 규칙 입력

⊖

⊖

⊖

⊖

⊖

⊕

Yara Rule 생성



### Yara Rule 편집

```
1 import "pe"
2
3 rule Test
4 {
5     strings:
6         $sig1 = "kernel32.dll"
7         $sig2 = "admin"
8         $sig3 = "root"
9         $sig4 = "sudo"
10        $sig5 = "crack.exe"
11    condition:
12        $sig1 or $sig2 or $sig3 or
13        $sig4 or $sig5
14 }
```

Yara Rule 내 컴퓨터 다운로드    Yara Rule 플랫폼 업로드

조건 입력 시 탐지규칙 생성

- 문자열을 입력하면 탐지규칙을 생성 및 편집 가능
- 플랫폼 내 저장하거나 내 기기로 다운로드 기능 제공

01 규칙 문자열 입력

02 탐지규칙 생성

Platform GIPS

Apply Yara Rule

### Yara Rule 적용

- 1 Yara Rule 선택
- 2 비교 대상 파일 업로드
- 3 결과 확인

#### Yara Rule 선택

플랫폼 내 생성 Yara Rule    새로운 Yara Rule 업로드

- 5/16/2024, 1:49:58 PM  
rule\_93daa962-9893-4e51-ba1a-be817eba0a70.yar
- 5/16/2024, 2:18:41 PM  
rule\_8ad406bc-c13c-4c93-9271-10f5ed190192.yar
- 5/17/2024, 2:50:24 AM  
rule\_04002f5b-0907-4c65-98ab-aebfcae009f2.yar
- 5/20/2024, 3:06:09 PM  
demo.yar
- 5/20/2024, 10:39:45 PM  
rule\_b602c109-b1b8-4e71-affe-7ff4458879ad.yar
- 5/21/2024, 11:52:35 PM

#### 선택한 Yara Rule

```
1 import "pe"
2
3 rule test1
4 {
5     strings:
6         $sig1 =
7             "SSSSSSSSSSSSTTTTTTTTT:kk^L"
8         $sig2 = "8t2SCn"
9         $sig3 = "o!W\`0m"
10        $sig4 = "3pCG(H"
11        $sig5 = "Description"
12        $sig6 = "cDefE!gYjjiiij2mnop"
13        $sig7 = "ReadFile"
14        $sig8 = "GetProcAddress"
15        $sig9 = "w{|>d3"
16        $sig10 = "TSearchRec"
17        $sig11 = "FindClose"
18        $sig12 = "advapi32.dll"
```



Platform GIPS

Apply Yara Rule

### Yara Rule 적용

- ✓ Yara Rule 선택
- 2 비교 대상 파일 업로드
- 3 결과 확인

분석을 원하는 파일을 끌어오거나 [클릭](#)해 업로드해주세요.

51개

- b3de05b73e2f53ea18a5c4a5f6c28fb0 [0.22MB] × 삭제
- b3dedfa844e7f6f13672fcfa0911e309 [0.3MB] × 삭제
- b3e5f6692b1e6d74be822acbb05aa550 [0.25MB] × 삭제

업로드 하기

< 이전    다음 >

01 적용시킬 탐지규칙 선택

02 검사할 파일 업로드

Apply Yara Rule

## Yara Rule 적용

Yara Rule 선택      비교 대상 파일 업로드      3 결과 확인

전체 검사 대상파일

378개

매치된 파일	매치되지 않은 파일
b1dd2a23a53304a32b9ccc7a40968934 b3a041de4fb21e95e72c77efe69932e0 aff2d4fd1b5bc7884fc7ed356e2e32a0 afd2b81cadff3241574c6a7a53db2410 af451f79a93533f8d260206bcda9b6f0 b2ed9d272c8d9acc61553c79be86ae50 b00a398ca229020bf1fc5a6500725520 b2caf326bcfdd8231a3cf827f9a4fa10 af0e3df56c1bb55f5b350ec7853b2920 b0b7bba29e5f1bf0a0827f80cccdaa30 afc93d09d32d0e3c96399dbb14854e0 af59c924e9d160f082c05a9673187be0 b0cc132348e956c139b225b3cac58660	af7910bdcf1bb09c827117e121a582e0 afda6cfec45ded34d2a52b84ffe01410 b2c3971977559e3176371e0daf9f5210 b1cf11cc7b5a8b36c04d848d4ba64a80 b0cca7e10f43dcbcd681304d86e456d0 afb4f88a8ec97582eef99a1728e48d60 af789c5555038ade0ffd07e0a2eda220 b3d69dec94cb4767cac1863579d13f40 b0b392523d9573e66495293ee4b47b30 afcfae16ffedc9a70a77a37e9a632b50 b4b58143e83a4c4412d8b0432175e3d0 afe9f25d228a84e251052d2edbdab580 af79c50d6c58494d000f9684ef2e02d0

탐지규칙이 적용된 악성파일 분류

탐지규칙을 통과한 정상파일 분류

### 03

## 분류 적용 결과 확인

- 선택한 탐지규칙을 적용하여 정상/악성파일 분류

## 적용 결과 검증 진행

Cisco의 오픈소스 백신 소프트웨어 ClamAV \*, 국산 백신프로그램인 하우리의 바이로봇에서 탐지하지 못한 악성 파일도 탐지하는 우수한 성능 검증 완료

### 테스트 악성파일

정보보호연구실 보유  
악성 실행파일 Dataset

총 2종류의 악성파일 3개

Trojan	facc
W64/ lpamor.A	cf56 ff81

### 오픈소스 백신 SW - ClamAV

```
2024-34/PE/datasets/demo_mal$ clamscan ./
L/cf5673bec06d5eeb10a8a455a6257640: OK
L/facc1b29c250b25ff47fbc1986b3af60: OK
L/ff81ff6b7ef7930be59820348b5236a0: OK

----- SCAN SUMMARY -----
Known viruses: 8693043
Engine version: 0.103.11
Scanned directories: 1
Scanned files: 3
Infected files: 0
Data scanned: 2.91 MB
Data read: 2.74 MB (ratio 1.06:1)
```

악성 파일 미탐(탐지실패) > 정상파일로 탐지

### PLATFORM GIPS

#### Yara Rule 적용

Yara Rule 선택

전체 검사 대상파일

3개

매치된 파일

cf5673bec06d5eeb10a8a455a6257640  
ff81ff6b7ef7930be59820348b5236a0  
facc1b29c250b25ff47fbc1986b3af60

악성 파일 정탐(탐지성공) > 악성파일로 탐지

\* <https://www.clamav.net/>

Platform GIPS

Analyze PE File

### 단일 PE 파일 분석

분석을 원하는 파일을 끌어오거나 **클릭**해 업로드해주세요.

b4d2b35e3a537acaba7af33d818b0f90 **삭제**

**분석하기**



Platform GIPS

### 분석 파일 기본 정보

파일명  
b4d2b35e3a537acaba7af33d818b0f90

파일크기  
0.64MB

파일 마지막 수정일  
5/22/2024, 1:55:17 PM

### 공격 개수

16개

### 주요 사용 라이브러리

GDI32.DLL SHELL32.DLL US

### 헤더 영역 분석 시각화

DOS HEADER
DOS STUB
Signature 0x50450000 Machine

Platform GIPS

### 스트링 영역 분석

번호	추출 텍스트	공격/정상
1	;/vda	공격
2	2m+-'3	공격
3	{mo?f&	공격
4	zh&wp}m	공격
5	getmur	공격
6	wqct q!	공격
7	#]q)/=j	공격
8	h!bt7!2	공격
9	befj<z0	공격
10	qwn,n#	공격

Platform GIPS

### 헤더 영역 분석 시각화

GDI32.DLL

Signature 0x50450000
TimeDateStamp
# NumberOfSymbolTable
Magic Major/MinorLinker
SizeOfInitializedData
AddressOfEntryPoint
BaseOfData
SectionAlignment
MajorOSVersion MinorOSVersion
MajorSubsystemVersion MinorSubsystemVersion
SizeOfImage
Checksum
SizeOfStackReserve
SizeOfHeapReserve
LoaderFlags
ExportTable
ImportTable
ResourceTable
ExceptionTable
CertificateTable
BaseRelocationTable
Debug
GlobalPtr

Platform GIPS

### 헤더 영역 분석 시각화

Standad COFF Fields

번호	이름	값	Readable Value
0	Magic	267	267
1	Major/MinorLinker Version	6/0	6/0
2	SizeOfCode	143360	143360
3	SizeOfInitializedData	524288	524288
4	SizeOfUninitializedData	0	0
5	AddressOfEntryPoint	651264	651264
6	BaseOfCode	4096	4096
7	BaseOfData	126976	126976

01

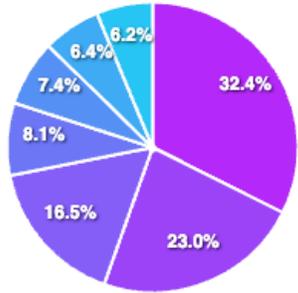
분석할 파일 업로드

02

파일 내 공격 문자열 및 개수, 헤더 영역 분석 결과 시각화

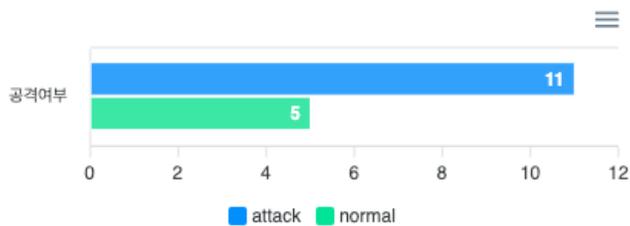
파일을 분석하여 악성 여부 판단 정보 제공

탐지 시그니처 비율



● trickler ● \share\_temp ● gistry ● ware\m ● ie 5.0 ● cxsocket ● gator.com

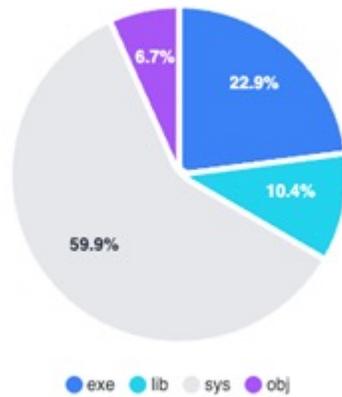
공격 탐지 비율



주요 탐지 시그니처



탐지 파일 종류



플랫폼 내에서 탐지한 여러 파일 정보의 통계값을 시각화하여 효과적으로 전달

- 보안 관리자가 통계 정보를 확인후 적절한 대응을 계획할 수 있도록 구성
- 주요 탐지 시그니처 비율
- 분석 대상 파일 중 공격 비율
- 탐지 파일 종류, 시그니처 워드클라우드

- 테스트 환경을 먼저 구축 후 실효성 검증필요
  - 테스트 데이터셋을 만들어 개발 초기 실험 환경을 구축함
  - 이후 연구실에서 보유하고 있는 악성파일 데이터셋을 적용하여 검증 완료
- 완성도를 높이기 위해서는 웹(UI) 구축, 시각화 도출 필요
  - 핵심 기술 개발 뿐만 아니라 사용하기 편리한 웹 플랫폼 구축 완료
  - 다양한 방식의 시각화 기능로 효과적인 정보 전달
- 핵심이 되는 코어 기술 정리 필요
  - 발표 초반 핵심 기술에 대해 자세하게 설명
  - 슬라이드 5~7 참조

## 우수한 성능 검증

- 바이로봇과 ClamAV같은 백신 미탐지 악성파일 탐지

## 산업체 수요 기술 개발

- 산학협력으로 진행, 기업과 사회가 실제로 필요로 하는 기술 개발

## 선행 연구 기술 고도화

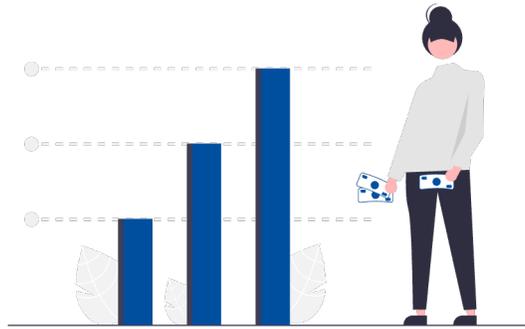
- 기존 네트워크 기반 선행 연구를 악성 코드에 적용해 고도화 기술 개발



## 기술적 효과

### 신속한 악성파일 식별 및 처리

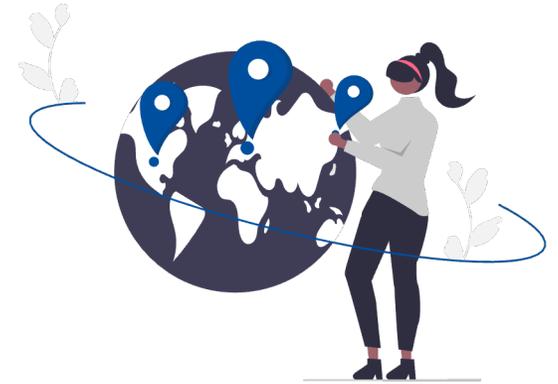
- 기업별 맞춤형 탐지규칙 생성 가능
- 보안수준 및 위협 대응 기술 고도화



## 경제적 효과

### 보안 전문인력 부족 해소

- 획기적인 오탐률 감소
- 자동 탐지 규칙 생성으로 효율적인 업무 가능



## 사회적 효과

### 신종공격으로 인한 사회적 피해 감소

- 증가되는 침해사고 예방 가능
- Zero-Day Attack 등 공격 대응 시간 저감

## 팀 구성원 후속 연구 과제 지속 참여 | 2024년 AI 보안 제품 및 서비스 사업화 지원사업



과학기술정보통신부



“생성형AI의 순기능과 역기능을 이용한 악성코드 야라를 자동 생성 및 공유 서비스”

### AS-IS

- 기술 검증을 위한 테스트 베드 환경 구축
- 시그니처 포함 기초 탐지 규칙

### TO-BE

- 악성 파일 처리를 위한 GIPS 변형 알고리즘 연구 개발
- 악성 코드 시그니처 그룹 생성을 위한 스트리밍 통계 처리 기술 개발

감사합니다



nurilab