

# PLATFORM GIPS

생성형 침입 방지 기술기반 보안 플랫폼

국민대학교 소프트웨어학부 2024 캡스톤디자인  
정보보호연구실 & (주)누리랩 | 산학협력 34조  
엄석현 김태경 김태윤 박준서 | 지도교수 윤명근



생성형 침입방지 기술 GIPS\*를 사용하여

다수의 악성 파일로부터  
공통된 시그니처를 추출후  
탐지 규칙을 생성하는  
보안 플랫폼



GIPS\*

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

## 프로젝트 소개



## 주요 기능

**추출 시그니처**

```

pf9c'c cgvff: kdvm/hxv5mk
trickler.inf d/l will be retried in %d seco
5f3cda6d n4gm'so uj'x'v9
runsetup: silentsetup completes, allowiv
system is online, delaying %d seconds.
7n8_by8 fe[3zme 7'727-74'
5.0.2014.213 키5[ 0@1000
5f50a3ac 5f50a3b1 ob-nf$
lugse 7%u+37 fssatofix
**** cancelled after dlg... ****
**forcing dropdead** $bnshh
    
```

**자동 생성 탐지 Yara Rule**

```

1 import "pe"
2
3 rule test1
4 {
5     strings:
6         $s1g1 = "pf9c'c" nocase
7         $s1g2 = "cgvff:" nocase
8         $s1g3 = "kdvm/hxv5mk1vhtgwxxya==" nocase
9         $s1g4 = "ffffffffff'fff" nocase
10        $s1g5 = "59d4de6e" nocase
11        $s1g6 = "<cfvcbch<" nocase
12        $s1g7 = "trickler.inf d/l will be retried
13        $s1g8 = "5wqid_" nocase
14        $s1g9 = "74,45(" nocase
15        $s1g10 = "rg1'l.u" nocase
16        $s1g11 = "t'pnjbn4" nocase
    
```

• **탐지규칙 생성&적용**  
파일 분석후 탐지규칙 자동 생성, 악성 탐지기능 제공

**분석 파일 기본 정보**

파일명: ce45ca3ac00cf9d9c2b3518242b8af0  
파일크기: 0.83MB  
파일 마지막 수정일: 5/23/2024, 1:46:16 AM

**공격 개수**  
775개

**주요 사용 라이브러리**

COMCTL32.DLL	GD32.DLL	NETAPI32.DLL	SHELL32.DLL
USER32.DLL	VERSION.DLL	WINNET.DLL	WSOCK32.DLL

**스트링 영역 분석**

번호	추출 텍스트	공격 정상
771	tidmessagepartsp	공격
772	<'c3@<cr-cvc	공격
773	6<6d8h6j6d6	공격
774	(tortusshelchangenotifierrenametevent	공격
775	;C=Z=>=	공격
776	wsasendto	정상
777	getastactivepopup	정상

• **악성 파일 분석**  
업로드한 파일의 악성여부 검사, 분석정보 제공

**탐지 시그니처 비율**

**탐지 파일 종류**

**공격 탐지 비율**

**주요 탐지 시그니처**

```

trickler.inf d/l will be retried in %d seconds
5f3cda6d n4gm'so uj'x'v9
runsetup: silentsetup completes, allowiv
system is online, delaying %d seconds.
7n8_by8 fe[3zme 7'727-74'
5.0.2014.213 키5[ 0@1000
5f50a3ac 5f50a3b1 ob-nf$
lugse 7%u+37 fssatofix
**** cancelled after dlg... ****
**forcing dropdead** $bnshh
    
```

• **탐지통계 시각화**  
플랫폼 내 분석한 정보를 다양한 형태로 시각화

## 기대 효과

**01 기술적 효과**  
신속한 악성파일 식별 및 처리  
기업별 탐지규칙을  
이용한 보안수준 고도화

**02 경제적 효과**  
보안 전문 인력 부족 해소  
획기적인 오탐률 감소  
효율적인 인력 운영가능

**03 사회적 효과**  
신종 공격으로 인한 사회적 피해 감소  
Zero-Day Attack 등  
신종 공격 대응시간 저감

## 주요 성과

**01 우수한 성능 검증**  
• 오픈소스 백신 SW (ClamAV)에서 미탐지된 악성파일도 정상탐지

**02 산업체 수요 기술 개발**  
• 산학협력으로 진행하며 기업과 사회가 필요로 하고 있는 주제로 개발

**03 선행 연구 고도화**  
• 기존 네트워크 기반 선행 연구를 악성코드에 적용해 고도화 기술 개발

## 후속 계획

**팀 구성원 후속 산학협력 연구 개발 지속 참여 예정**

과학기술정보통신부 KISA 한국인터넷진흥원

2024년 AI 보안 제품 및 서비스 사업화 지원사업

**악성 실행 파일 처리를 위한 GIPS 변형 알고리즘 연구 개발**  
악성코드 시그니처 그룹 생성을 위한  
스트리밍 통계 처리 기술 개발