부산대학교 제로트러스트 클라우드 보안 연구센터

제로트러스트 클라우드 보안 연구센터 ZeroTrust Cloud Security Research Center

웹쉘 맞춤 TextRank 알고리즘을 이용한 난독화된 PHP 웹쉘 탐지

머신러닝 알고리즘 및 TextRank 알고리즘 기술을 활용한 난독화 웹쉘 탐지 기술

적용 분야

클라우드 보안 | 디지털 포렌식 | AI 보안

침입 탐지 | 정보유출 방지 | 보안 위협 분석

연구 목적

▸ 기존 방식 : 정적 웹쉘 탐지 도구에서 탐지가 어려운 난독화된 웹쉘에 대한 탐지 성능을 향상 시키면서, 일반 난독화 파일 또한 정확히 분류할 수 있는 기술을 개발

▸ 제안 하는 방식 : 웹쉘 탐지에 적합한 전처리 기술 개발을 통한 웹쉘 탐지 기술의 정확도를 향상 시키고 난독화 웹쉘 특징 추출에 효율적인 기술 개발을 통해 탐지 시 발생할 수 있는 오탐 감소시키는 기술을 제안함

<일반 데이터의 난독화 및 난독화 데이터의 정상/웹쉘 여부 탐지 결과 예시>

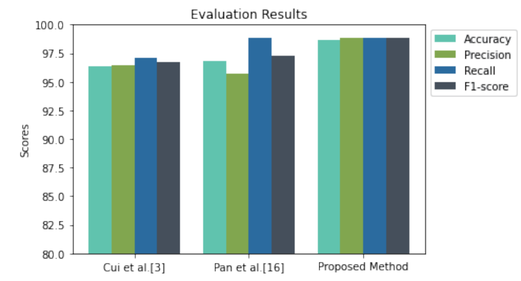
```
<?php
$x=base64_decode("YX
NzZXJ0");
$x($_POST['c']);?>
```

일반 데이터

난독화

```
<?php
$x = "assert";
assert($_POST['c']);
```

난독화 데이터



탐지 결과 분석

연구 내용

① 웹쉘 탐지를 위한 전처리 기술 개발

▸ AST/Opcode 를 활용한 웹쉘 전처리 기술 개발

② 난독화 웹쉘 특징 추출을 위한 알고리즘 개발

▸ 비난독화 기술 적용

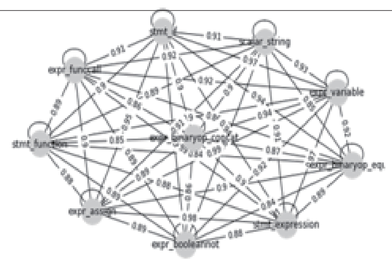
▸ 웹쉘 탐지를 위한 웹쉘 맞춤 TextRank 알고리즘 개발

③ 난독화 웹쉘 탐지를 위한 머신러닝 모델 연구

④ 관련 최신 연구 분석 및 오탐 결과 분석 비교

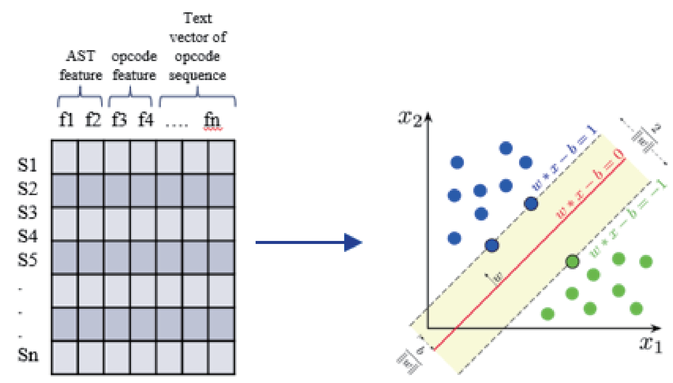
<제안하는 난독화 웹쉘 탐지 기술 >

AST	Count
Expr_funcall	57325
Stmt_Expression	109077
Stmt_do	34
Stmt-Goto	5



웹셀 주요 특징 추출 알고리즘 연구

난독화된 웹쉘



난독화 웹쉘 분류 기법 연구

기술 경쟁력

기존기술	기술 차별성	대상기술
• 웹쉘 탐지 시, 단순 통계적 방식으로 인한 낮은 정확도 • 난독화된 웹쉘 탐지 시, 데이터 편향으로 인한 오탐 발생		• 웹쉘 탐지 시, 기존 기술 대비 높은 정확도 • 난독화 웹쉘 탐지 시 발생할 수 있는 오탐률 감소
기술적 한계 ▸ 기존 정적 웹쉘 탐지 기술의 경우, 단순 통계 기반의 특징 추출로 인해, 탐지 정확도가 떨어지는 문제가 발생함 ▸ 난독화 웹쉘 탐지에서 일반 난독화 파일도 웹쉘로 탐지해버리는 오탐 (False Positive)이 다수 발생함		**기술적 우위** ▸ 웹쉘 특성을 고려한 전처리 기술 개발을 통한 유용한 정보 추출 및 높은 탐지 성능 ▸ 난독화된 일반 파일 또한 고려한 알고리즘 적용을 통한 오탐 (False Positive) 감소

문의처 | 제로트러스트 클라우드 보안 연구센터 E. csrc@pusan.ac.kr T. 051. 510. 7212