

# Opcode와 API의 군집화와 유사도 분석을 활용한 랜섬웨어 탐지모델

2022.06.13

조장 이계혁

조원 황민채

조원 현동엽

발표자 구영인



산업과 예술의 만남

**홍익대학교** 세종



산업과 예술의 만남

홍익대학교 세종

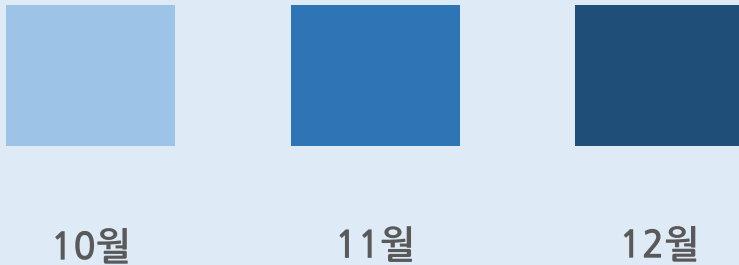
# Contents

- I. 서론
- II. 결과발표
- III. 초기 기계학습 모델 최적화
- IV. 원과 랜섬웨어 간 탐지결과
- V. 향후 계획

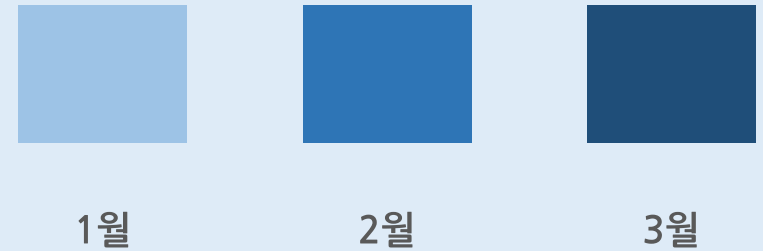
## 2. 서론

### 랜섬웨어 위협 지속 증가

#### 1 2021년 4분기 랜섬웨어 탐지 건수



#### 2 2022년 1분기 랜섬웨어 탐지 건수



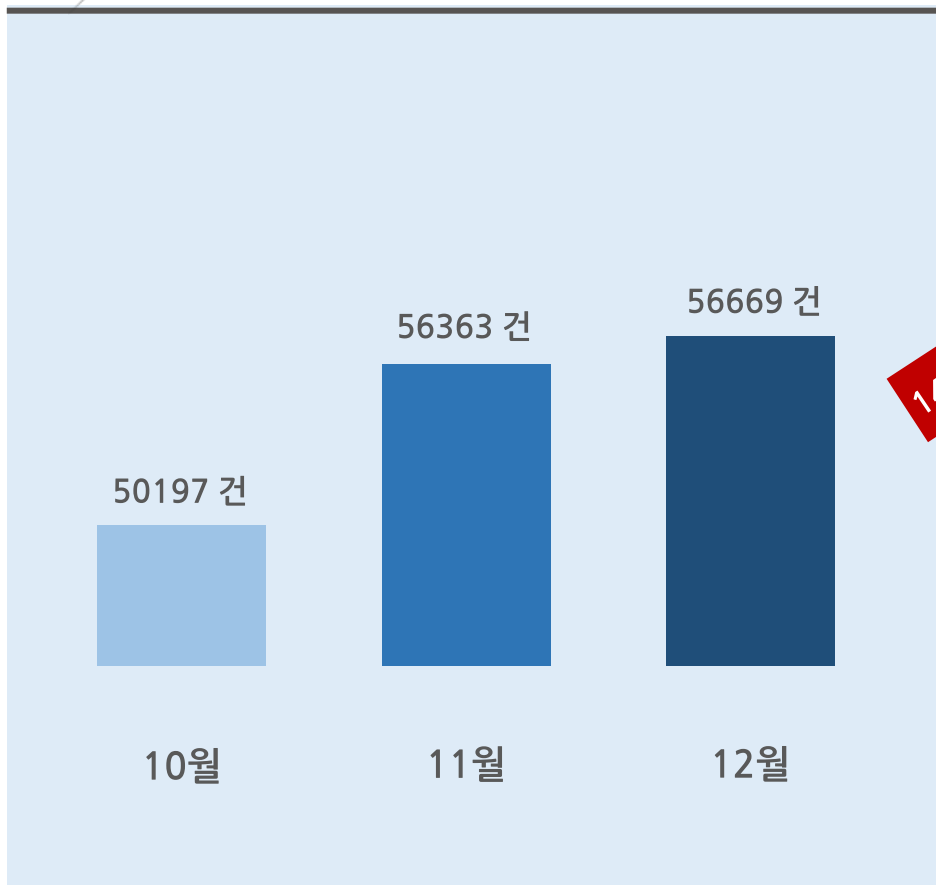
Ransomware Trends & Statistics, First Quarter for 2022, KISA



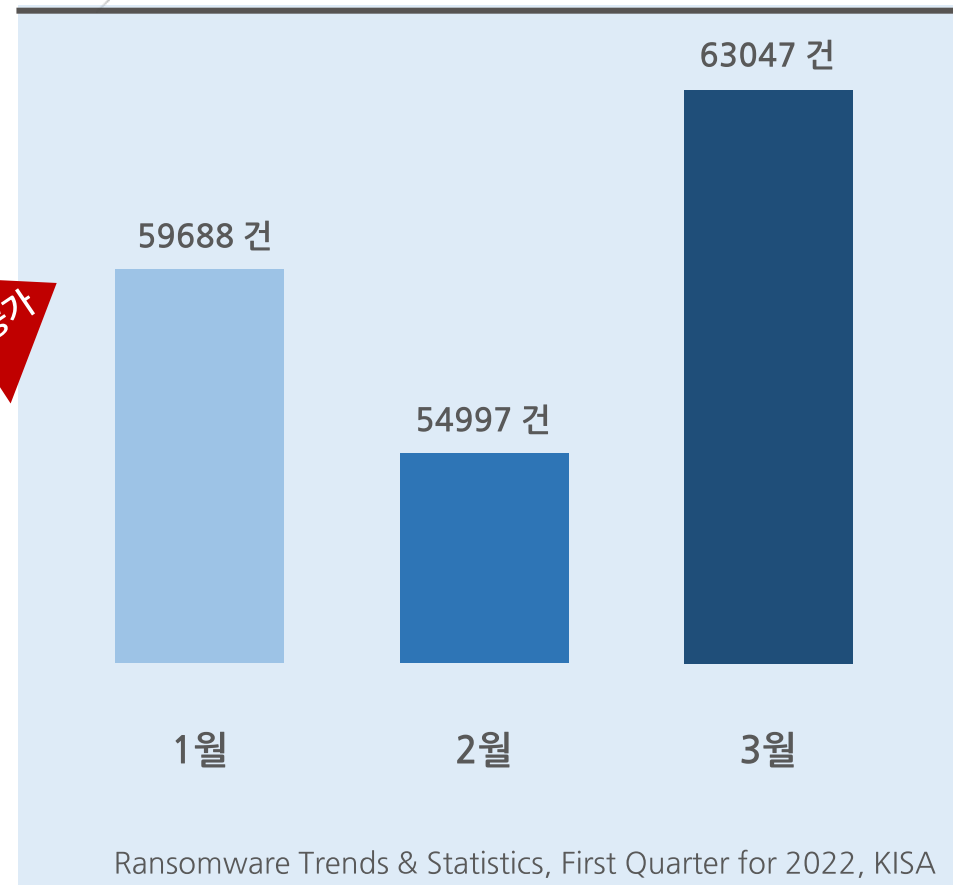
## 2. 서론

### 랜섬웨어 위협 지속 증가

1 2021년 4분기 랜섬웨어 탐지 건수



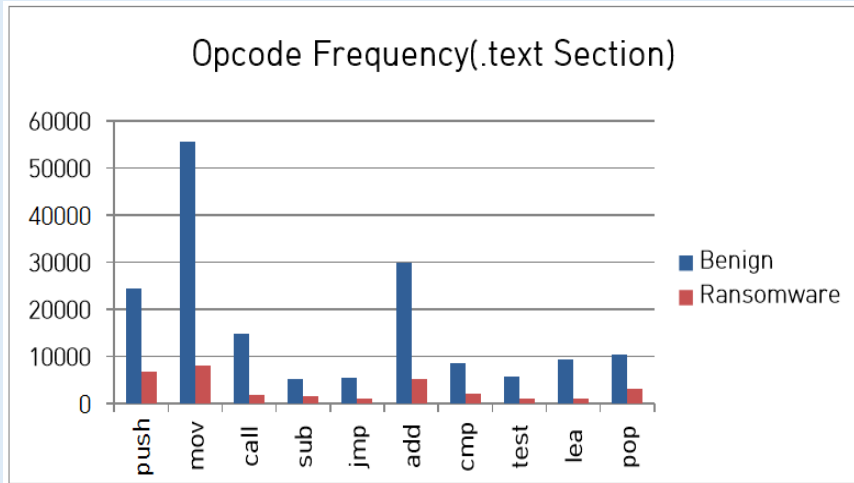
2 2022년 1분기 랜섬웨어 탐지 건수



## 2. 결과발표

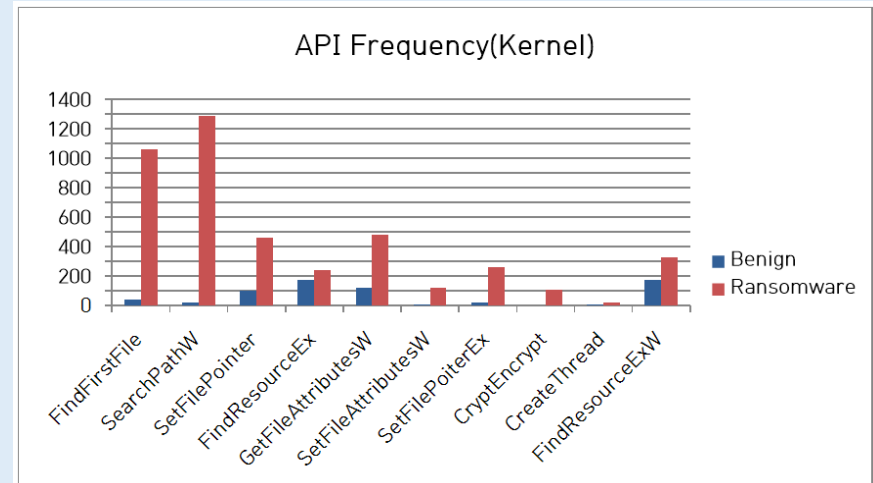
### 빈도수 분석으로 특징정보(Feature) 선정

#### 1 각 Opcode 항목 빈도수 그래프



- 총 10개의 .text Opcode 항목 빈도수를 파일 유형별로 비교 (push, mov, call, sub, jmp, add, cmp, test, lea, pop)
- 선정한 Opcode 항목의 빈도수가 **파일 유형별** **확연한 차이**를 가짐에 따라 특징정보로 사용될 수 있다고 추측할 수 있다.

#### 2 각 Native API 항목 빈도수 그래프

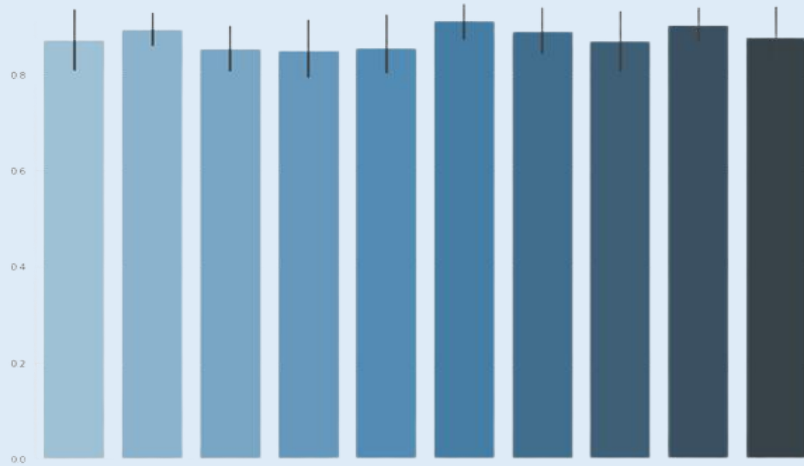


- 총 10개의 API 항목 호출 빈도수를 파일 유형별로 비교 (FindFirstFile, SearchPathW, SetFilePointer 등)
- 선정한 API 항목의 호출 빈도수가 **파일 유형별** **확연한 차이**를 가짐에 따라 특징정보로 사용될 수 있다고 추측할 수 있다.

## 2. 결과발표

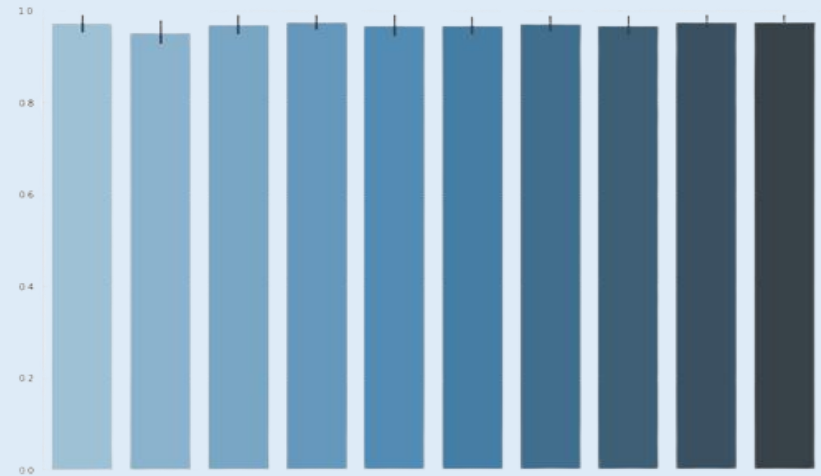
### 항목별 랜섬웨어 파일 코사인 유사도 분석

#### 1 Opcode 항목별 빈도수 코사인 유사도



- 앞서 선정한 총 10개 Opcode 항목의 빈도수를 기반으로 랜섬웨어 실행파일 간 코사인 유사도(Cosine Similarity) 측정
- 0.8에서 0.9사이의 값 도출, 해당 특징정보(Feature)가 기계학습의 독립변수로 사용될 수 있다.

#### 2 API 항목별 호출 빈도수 코사인 유사도

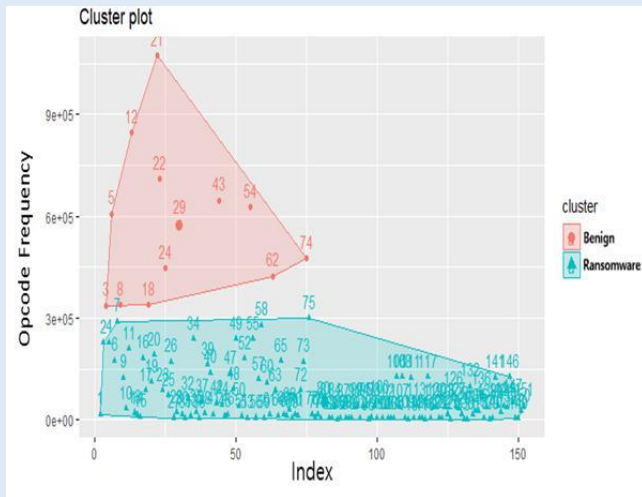


- 앞서 선정한 총 10개 API 항목의 호출 빈도수를 기반으로 랜섬웨어 실행파일 간 코사인 유사도(Cosine Similarity) 측정
- 평균 0.9 이상의 값 도출, 해당 특징정보(Feature)가 기계학습의 독립변수로 사용될 수 있다.

## 2. 결과발표

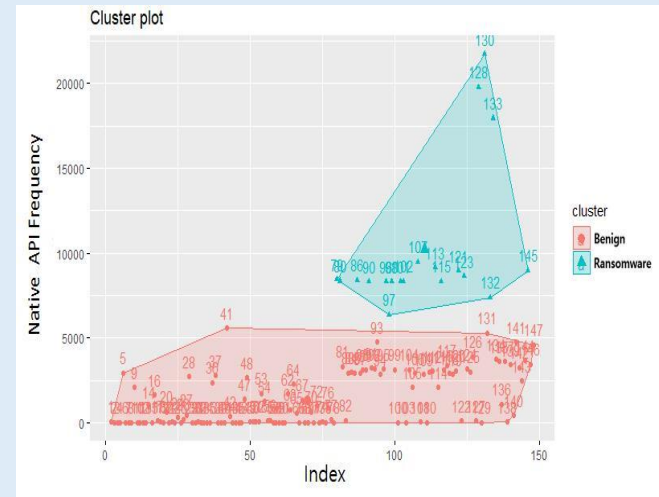
### 파일 유형별 클러스터링 분석으로 군집화

#### 1 파일 유형별 Opcode 빈도수 군집화



- K=2로 설정, 총 2개의 군집으로 클러스터링(Clustering) 검증
- 선정한 Opcode 항목의 빈도수를 기반으로 군집 형성, 정상 실행파일과 특정 랜섬웨어 실행파일의 뚜렷한 군집 확인

#### 2 파일 유형별 API 호출 빈도수 군집화




- K=2로 설정, 총 2개의 군집으로 클러스터링(Clustering) 검증
- 선정한 API 항목의 호출 빈도수를 기반으로 군집 형성, 정상 실행파일과 특정 랜섬웨어 실행파일의 뚜렷한 군집 확인

## 2. 결과발표

### 두 분석정보의 결합과 기계학습 결과

#### 1 두 분석정보의 결합

선정	선정한 10개 Opcode 항목의 <b>파일 유형별 Frequency 비교</b> 를 통한 특징정보(Feature) 선정
검증	Cosine Similarity 검증 및 Clustering 검증으로 선정한 항목의 파일 유형별 유의미한 차이 입증
선정	선정한 10개 Native API 항목의 <b>파일 유형별 호출 Frequency 비교</b> 를 통한 특징정보(Feature) 선정
검증	Cosine Similarity 검증 및 Clustering 검증으로 선정한 항목의 파일 유형별 유의미한 차이 입증
	
검증	피어슨 상관계수 검증으로 두 분석정보 간 $-0.3 < r < -0.1$ 의 음(-)의 상관관계를 가짐
결합	피어슨 상관계수 검증결과, 두 분석정보 간 <b>반비례의 특성(-)</b> 을 가짐에 따라 항목을 더하여 결합

#### 2 탐지모델 기계학습 초기 결과

N/Depth	Accuracy	Precision	Recall	F1-Score
20/5	93.54%	100%	88.8%	94.1%
100/20	96.77%	100%	94.11%	96.9%
100/100	96.77%	100%	94.11%	96.9%

#### Random Forest Evaluation

Cost	Accuracy	Precision	Recall	F1-Score
C = 1	87.0%	100%	77.7%	87.5%
C = 3	87.0%	92.8%	81.2%	86.7%
C = 8	87.0%	92.8%	81.2%	86.7%
C = 100	83.8%	92.8%	76.4%	83.8%

#### SVM Evaluation



# 3. 초기 기계학습 모델 최적화

## 초기 기계학습 모델 최적화

### 1 사용한 최적화 프레임워크



OPTUNA

- 최적의 조합, 파라미터 별 중요도를 판단하고 찾는다.
- 거의 모든 ML/DL에서 사용 가능하다.
- 간단하며, 연산속도가 빠르다.
- 다양한 최적화 알고리즘을 갖추고 있다.
- 내장된 함수로 시각화가 가능하다.

### 2 하이퍼파라미터 최적화 적용 개요

#### Random Forest Optimization

가장 높은 정확도를 얻는 N\_estimator 값 도출 및 적용

가장 높은 정확도를 얻는 Max\_depth 값 도출 및 적용

N\_estimator 값과 Max\_depth 값의 최선의 조합 도출

#### SVM Optimization

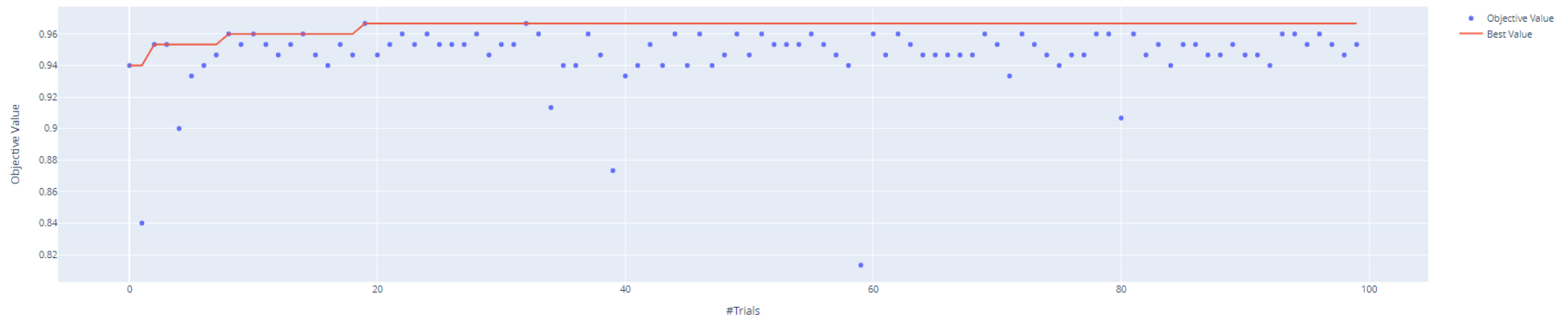
Cost 값의 최소범위와 최대범위를 임의 설정

가장 높은 정확도를 얻는 Cost 값 도출 및 적용

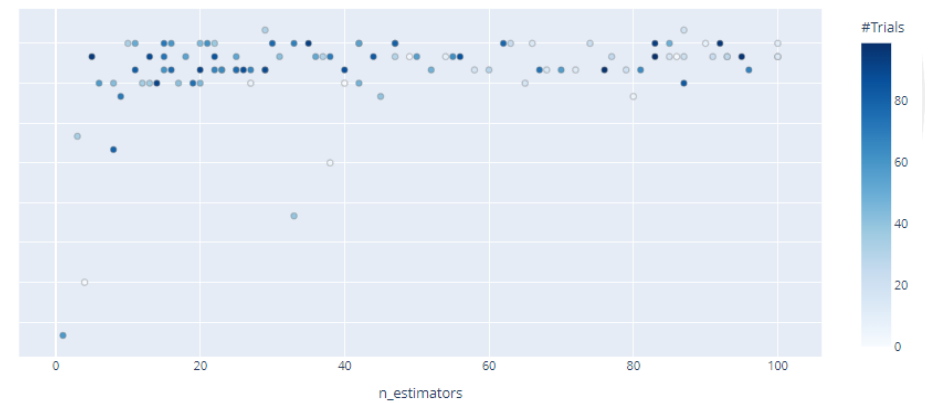
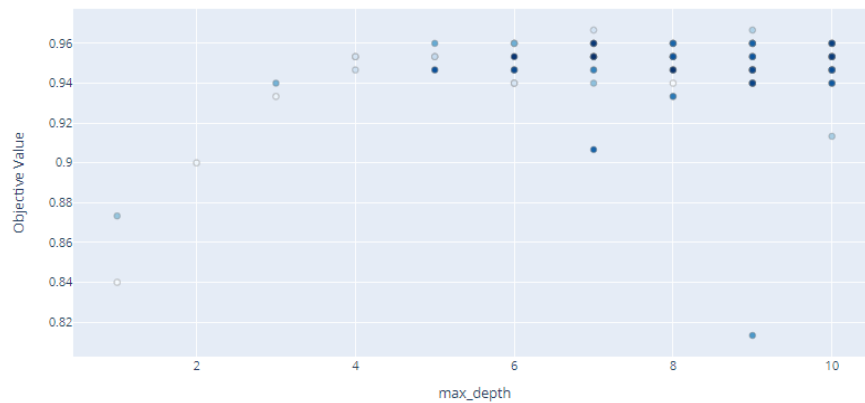
# 3. 초기 기계학습 모델 최적화

## RF 최적화 과정 Plot

Optimization History Plot



Slice Plot

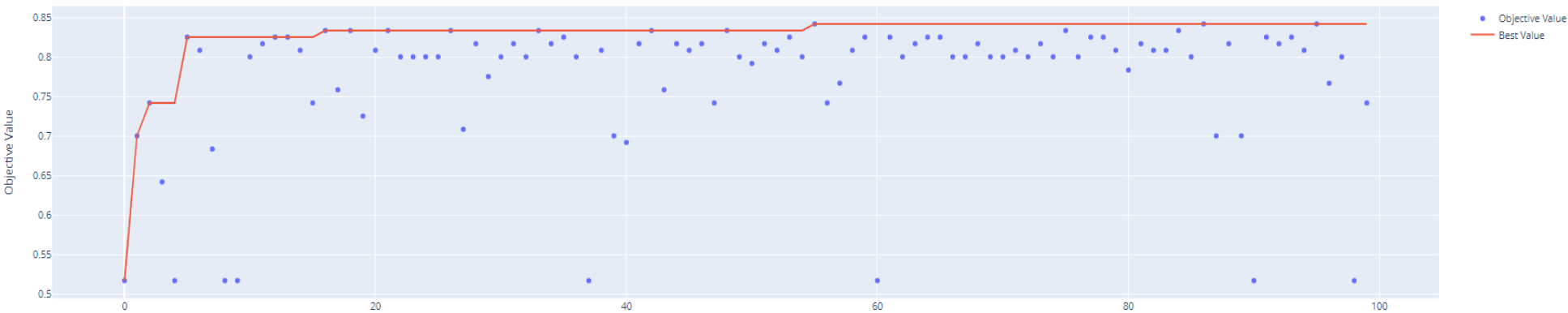


# 3. 초기 기계학습 모델 최적화

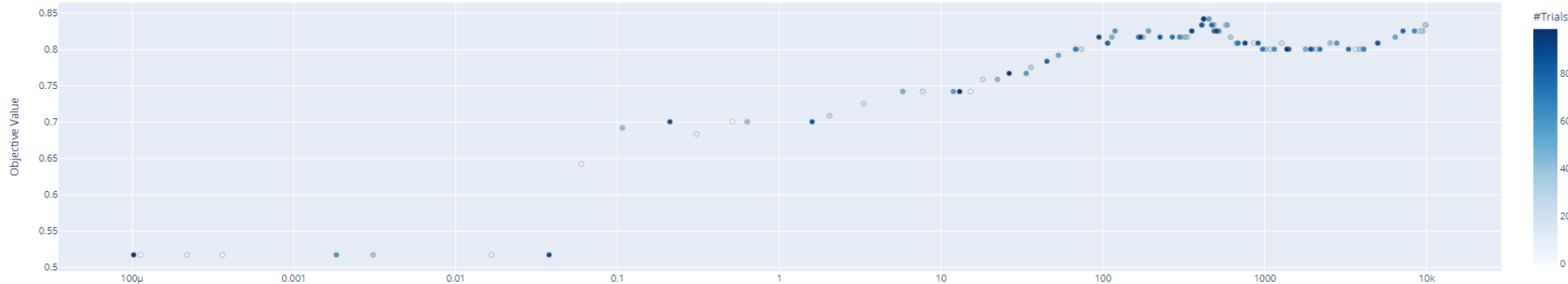


## SVM 최적화 과정 Plot

Optimization History Plot



Slice Plot



# 3. 초기 기계학습 모델 최적화

## 최적화 적용 후 초기모델 탐지 평가

### 1 Random Forest 최적화 결과

- N\_estimators 값과 Max\_Depth 값의 범위는 1 - 100 / 1 - 10으로 설정
- Accuracy : 0.9733333333333334 (Train Accuracy)  
Best hyperparameters :  
{‘n\_estimators’ : 43, ‘max\_depth’ : 9}



N/Depth	Accuracy	Precision	Recall	F1-Score
43/9	93.3%	92.8%	92.8%	92.8%

Validation Dataset RF Evaluation

### 2 SVM 최적화 결과

- Cost 값의 범위는 1e-4 - 1e4 (-10000,10000)으로 설정
- Accuracy : 0.8416666666666666 (Train Accuracy)  
Best hyperparameters :  
{‘C’ : 451.2193673484867}



Cost	Accuracy	Precision	Recall	F1-Score
451	93.3%	100%	85.7%	92.3%

Validation Dataset SVM Evaluation



# 4. 웜과 랜섬웨어 간 탐지결과

## 웜, 특정 랜섬웨어 기계학습 탐지결과

### 1 탐지모델 RF 기계학습 결과

N/Depth	Accuracy	Precision	Recall	F1-Score
20/5	97.4%	100%	93.3%	96.5%
100/20	100%	100%	100%	100%
100/100	94.8%	93.3%	93.3%	93.3%



Optimization

N/Depth	Accuracy	Precision	Recall	F1-Score
96/2	97.4%	93.7%	100%	96.7%

### 2 탐지모델 SVM 기계학습 결과

Cost	Accuracy	Precision	Recall	F1-Score
C = 1	89.7%	100%	73.3%	92.85%
C = 5	89.7%	86.6%	86.6%	86.6%
C = 10	82%	90%	60%	72%
C = 100	94.8%	100%	86.6%	92.85%



Optimization

Cost	Accuracy	Precision	Recall	F1-Score
139	94.8%	93.3%	93.3%	93.3%

- 특징정보는 앞서 선정한 Opcode 항목, API 호출 빈도수를 이용
- 특정 랜섬웨어 탐지 지표를 평가, 앞서 진행한 최적화 적용
- 선정한 특징정보가 다양한 유형의 바이러스에 해당되는 것이 아닌, 특정 랜섬웨어 탐지에 특화된 특징정보임을 확인할 수 있다.

Frequency	Percentage
Daily	45%
Weekly	35%
Monthly	15%
Other	5%

## Project Plan Time Table

No.	세부내용	~6월	7월	8월	9월	10월	11월	12월
1.	데이터 세트 구축 및 모델 성능 검증							
2.	모듈 개발 및 구현							
3.	모듈 테스트 및 통합 테스트							
4.	최종 논문 작성							
5.	모듈 패키징 및 응용 프로그램 개발 및 구현							
6.	최종 프로젝트 검토 및 학술제 발표							
7.	피드백 보완 및 추가 기능 연구							