Malware Analysis Project

김현수(Hyeonsu Kim)

최가온(Gaon Choi)

Contents

1. Previous works
2. Malware-image Transformation
3. Malware Binary Classification (malware or non-malware?)
4. Malware Family Classification
5. Other works




Introduction

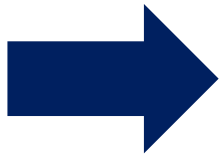
이번 프로젝트에서는 악성코드 파일을 이미지로 변환한 후,
이미지를 기반으로 악성 여부를 판단하고,
악성코드 계통(malware family)을 분류하는 인공지능 모델을
설계하고 학습하였습니다.

Previous works

지난 발표 시기까지의 프로젝트 진행 요약

Malware Image Visualization

imageio.imwrite



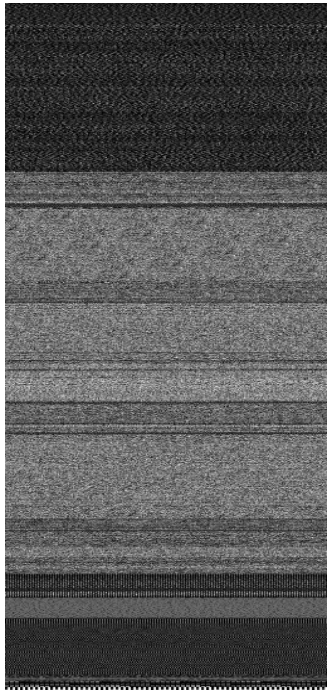
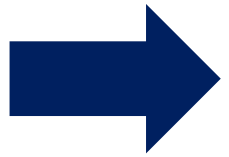
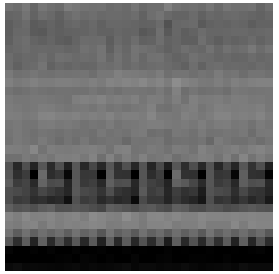


Image.resize(32,32)





.vir file

.png file

.png file

Binary classification training using VGGNet

malware: 500개, non-malware: 500개

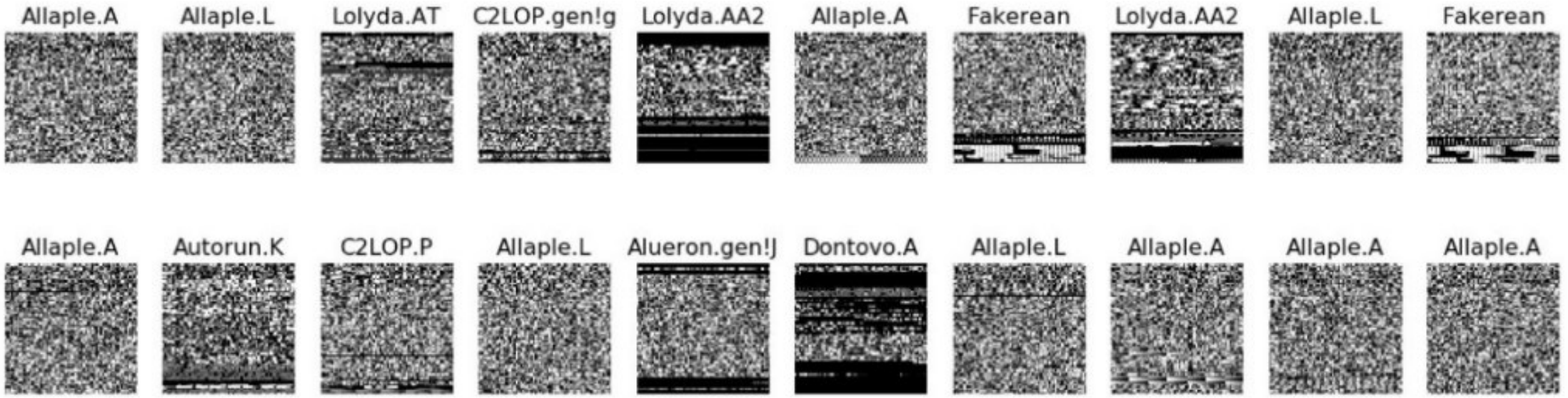
Layer(type)	Output Shape	# of params
con2d(Conv2D)	(None, 32, 32, 3)	84
activation (Activation)	(None, 32, 32, 3)	0
vgg16 (Functional)	(None, None, None, 512)	14714688
flatten (Flatten)	(None, 512)	0
dense (Dense)	(None, 32)	16416
dense_1 (Dense)	(None, 1)	33

Performance	
Train loss	loss: 0.0291
Train acc	accuracy: 97.87
Test loss	loss: 0.2332
Test acc	accuracy: 69.50

Malware Image Transformation

악성코드 파일 이미지화 및 데이터셋 분석

Malware Image Transformation



dataset	# of malware data points	# of non-malware data points
train set	7,000	3,000
test set1	5,000	5,000
test set2	5,000	5,000


Malware Binary Classification
악성여부 이진분류 모델 설계 및 학습

Malware Binary Classification

A model that receives a transformed 32 x 32 size image as input
and dichotomously determines whether it is malware or not(non-malware)

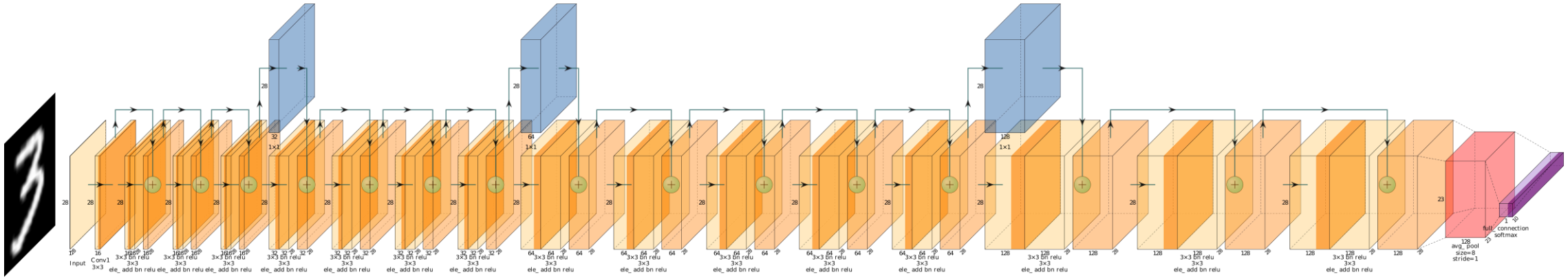
Malware Binary Classification

dataset	# of malware data points	# of non-malware data points
train set	7,000	3,000
test set1	5,000	5,000
test set2	5,000	5,000

dataset	# of malware data points	# of non-malware data points
train set	5,000	5,000
test set	5,000	5,000

Malware Binary Classification

ResNet50



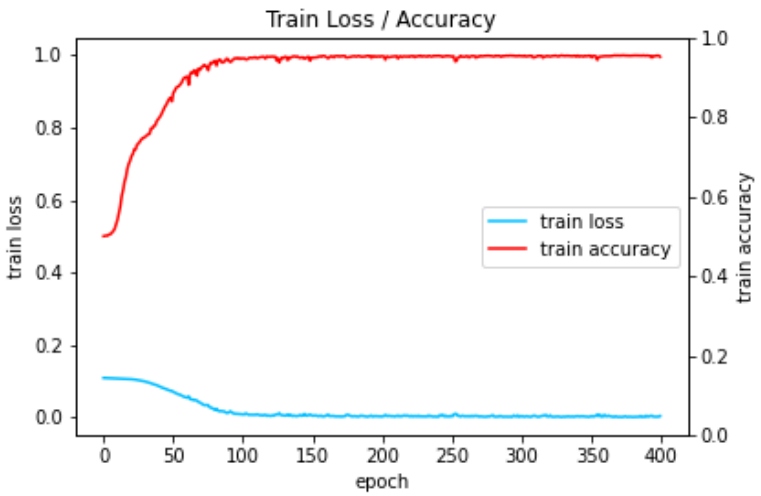
Malware or Non-malware?

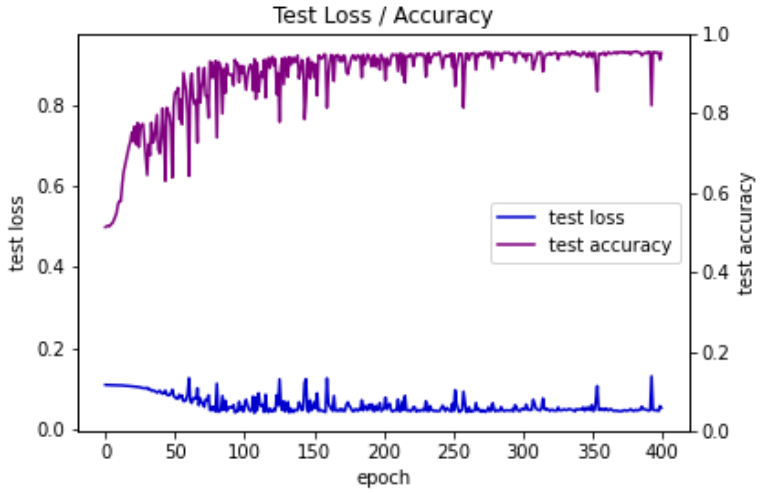
Binary Classification

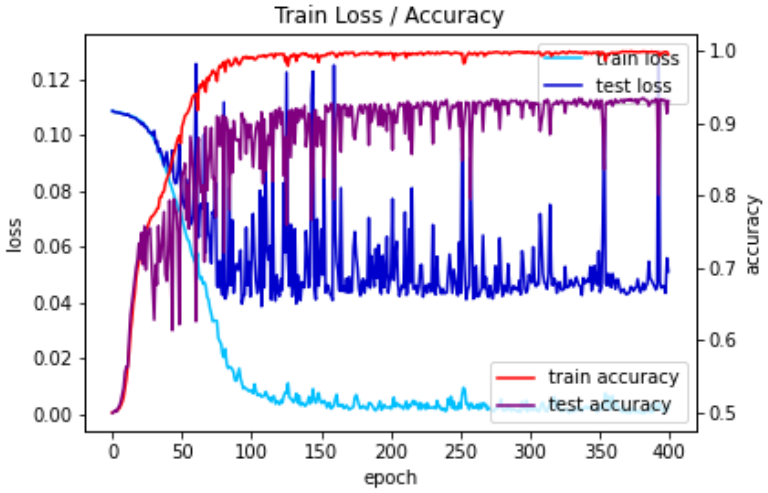
```
self.resnet_50.fc = nn.Sequential(
    nn.Linear(2048, 1000),
    nn.ReLU(inplace=True),
    nn.Linear(1000, 256),
    nn.ReLU(inplace=True),
    nn.Linear(256, 64),
    nn.ReLU(inplace=True),
    nn.Linear(64, 1),
    nn.Sigmoid()
)
```

Malware Binary Classification

Model Performance





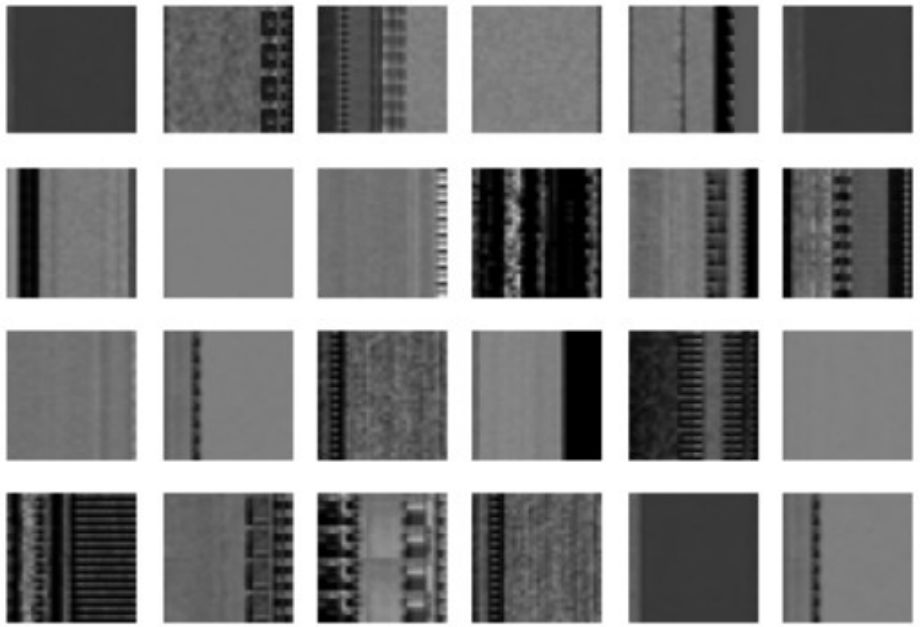


- Train Accuracy: 99.5%
- Test Accuracy: 93.0%
- Epoch: 400

- Learning rate: 0.001
- Loss: nn.BCELoss
- Optimizer: SGD

Malware Binary Classification

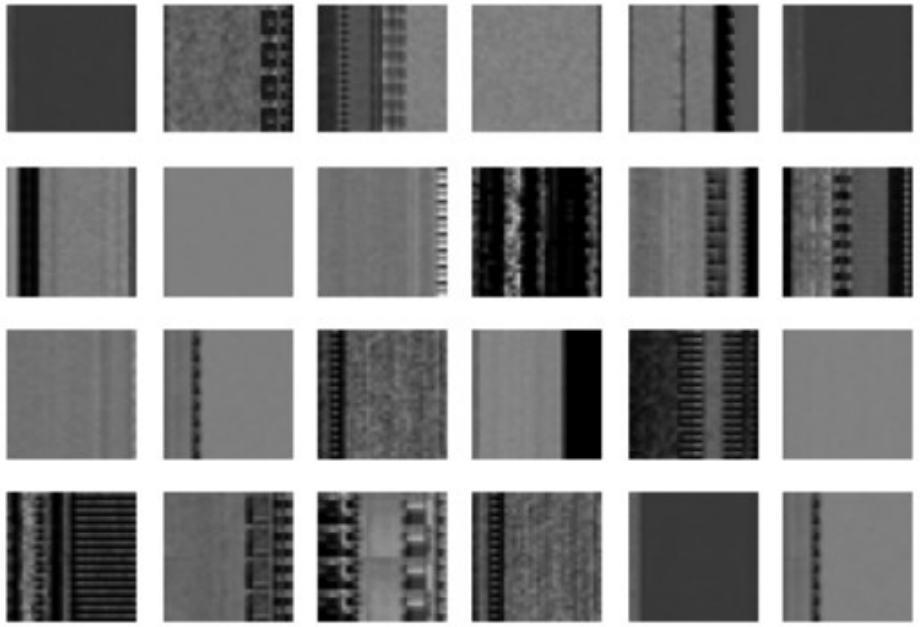
Model Performance

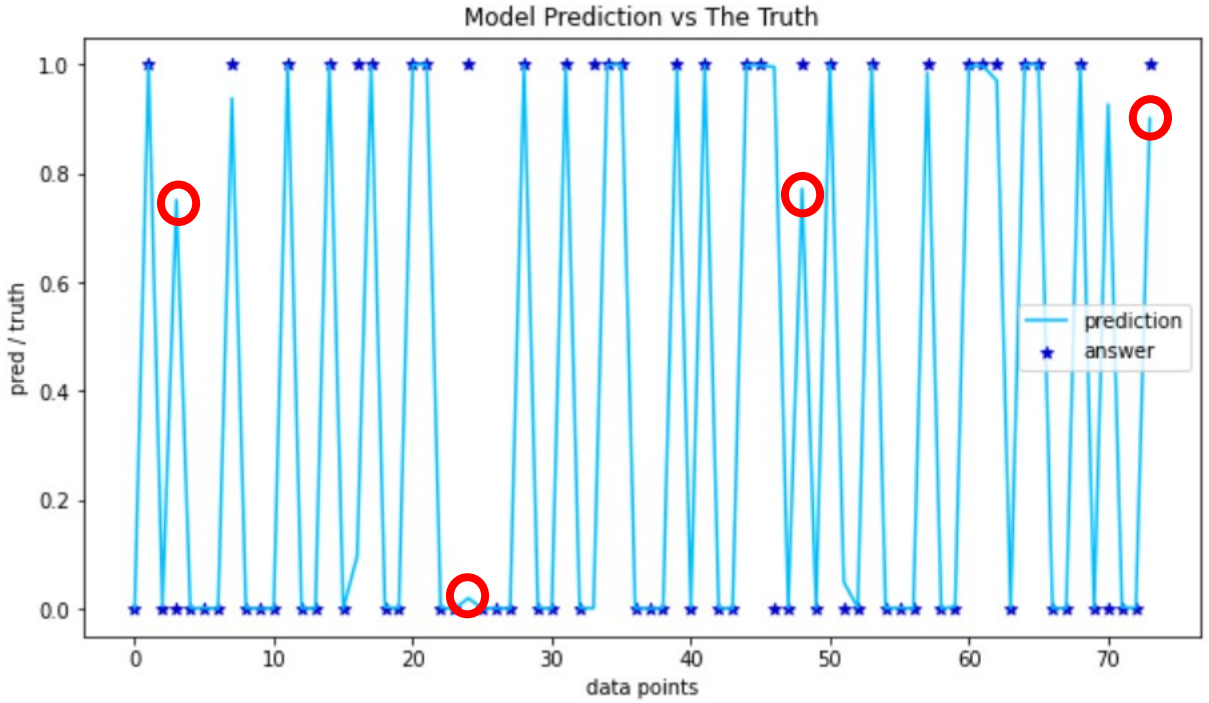


```
image 0 | pred=0.0014788481639698148 | ans=0
image 1 | pred=0.9997912049293518 | ans=1
image 2 | pred=0.005231290124356747 | ans=0
image 3 | pred=0.7512921690940857 | ans=0
image 4 | pred=0.0017309949034824967 | ans=0
image 5 | pred=0.001742606982588768 | ans=0
image 6 | pred=0.000600828614551574 | ans=0
image 7 | pred=0.9383810758590698 | ans=1
image 8 | pred=0.0016865450888872147 | ans=0
image 9 | pred=0.0007257546531036496 | ans=0
image 10 | pred=0.0006229666178114712 | ans=0
image 11 | pred=0.9989845156669617 | ans=1
image 12 | pred=0.001240861602127552 | ans=0
image 13 | pred=0.0006093949778005481 | ans=0
image 14 | pred=0.9991174340248108 | ans=1
image 15 | pred=0.00038419407792389393 | ans=0
image 16 | pred=0.0970044657588005 | ans=1
image 17 | pred=0.9984909296035767 | ans=1
image 18 | pred=0.00386615376919508 | ans=0
image 19 | pred=0.0015628642868250608 | ans=0
image 20 | pred=0.9997197985649109 | ans=1
image 21 | pred=0.9999942779541016 | ans=1
image 22 | pred=0.002477513626217842 | ans=0
image 23 | pred=0.0005884646088816226 | ans=0
```

Malware Binary Classification

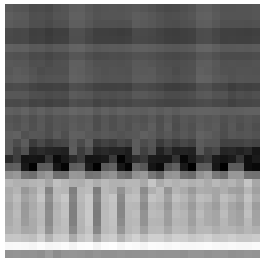
Model Performance

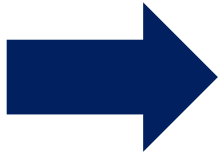


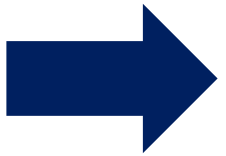



Malware Family Classification
악성코드 계통 분류 모델 설계 및 학습

Malware Family Classification







0: adware

1: downloader

2: dropper

...

A model that receives a transformed 32 x 32 size image as input and determines its malware family such as adware, downloader, etc.

Malware Family Classification

dataset	# of malware data points	# of non-malware data points
train set	7,000	3,000
test set1	5,000	5,000
test set2	5,000	5,000

dataset	# of malware data points
train set	7,000
test set1	5,000
test set2	5,000

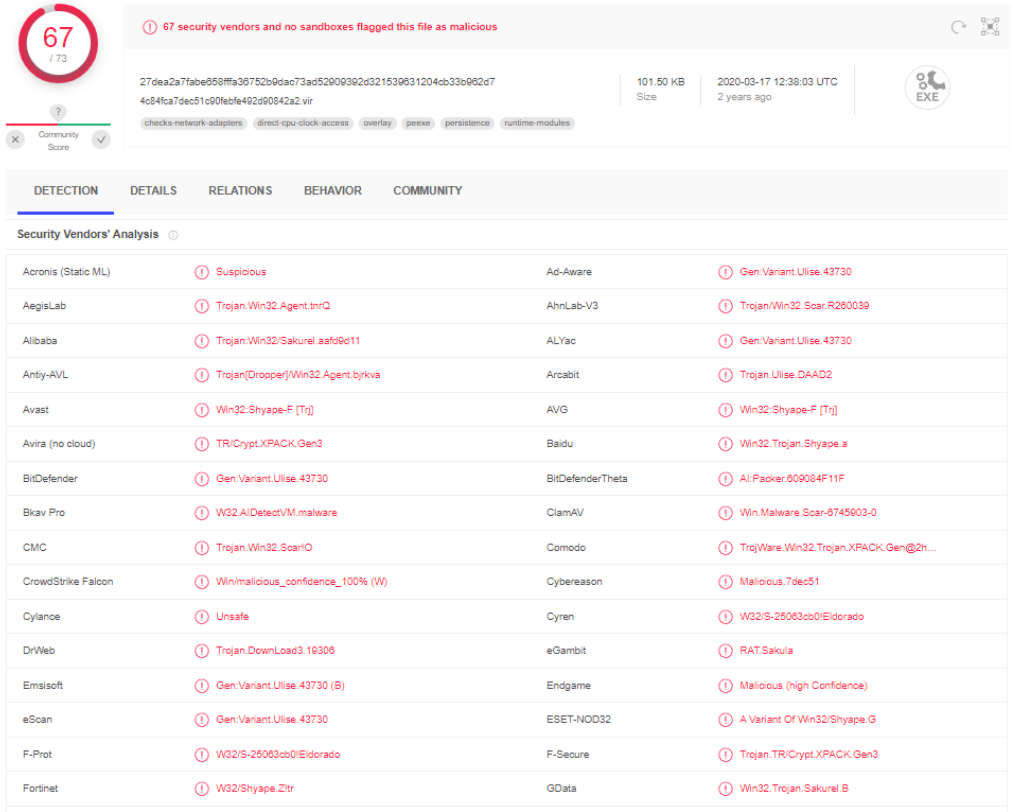
Malware Family Classification

dataset	# of malware data points
train set	7,000
test set1	5,000
test set2	5,000

dataset	# of malware data points
ALL	17,000

Malware Family Classification

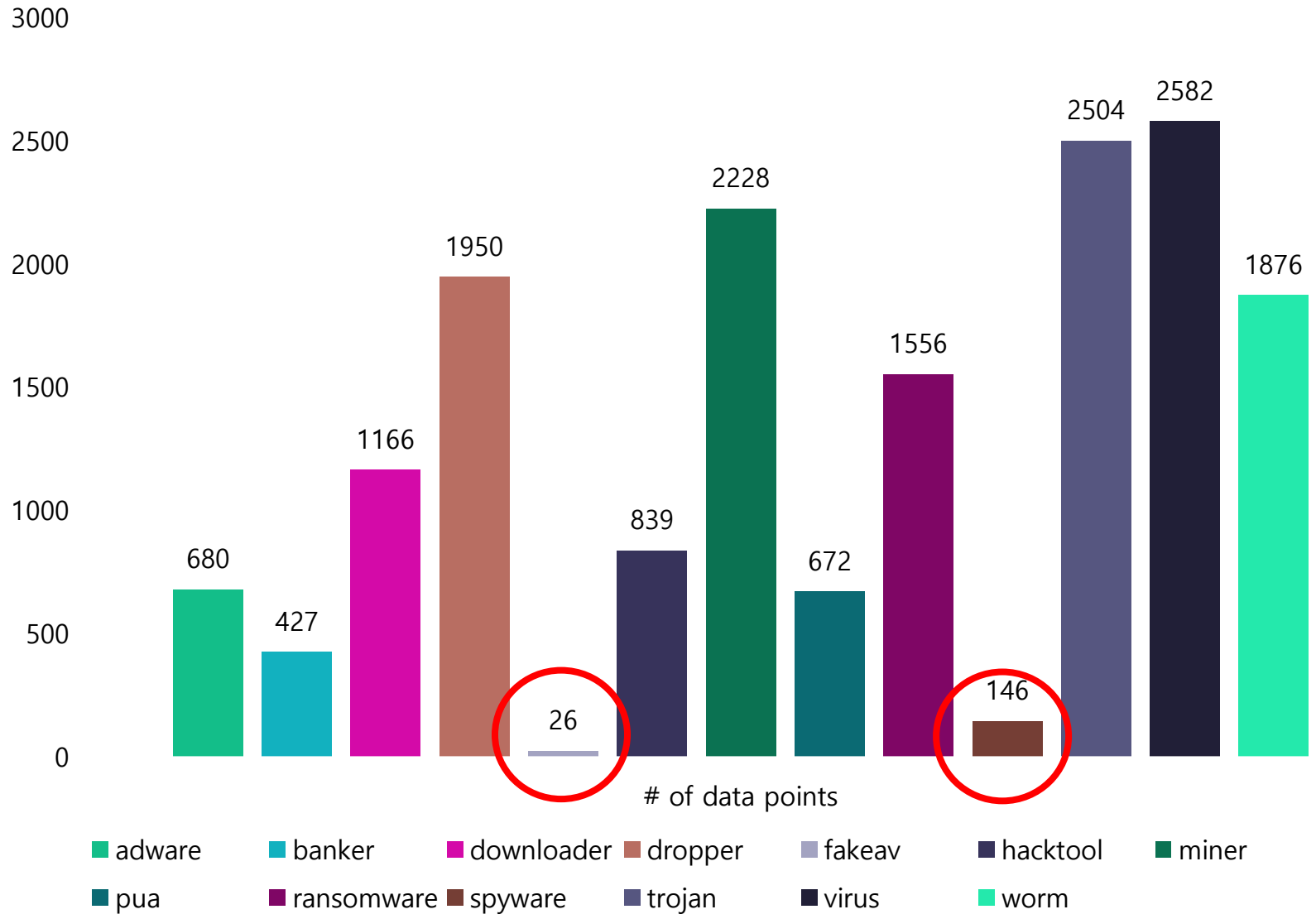
dataset	# of malware data points
ALL	17,000



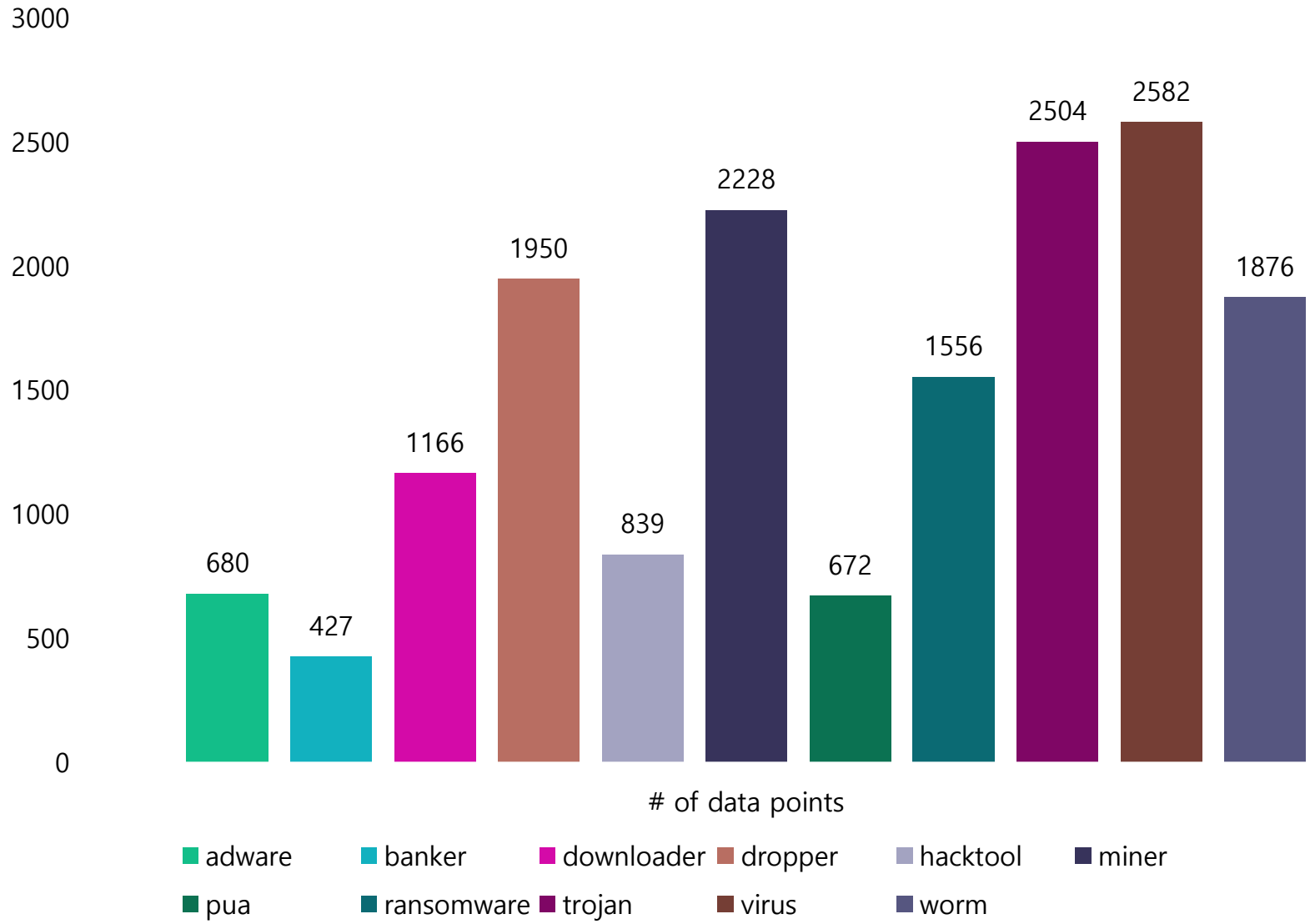
Extracts labels from examination data based on **VirusTotal**.

1. majority rule
2. exceptions for trojan
    1) only case -> trojan
    2) else -> get the 2nd decision

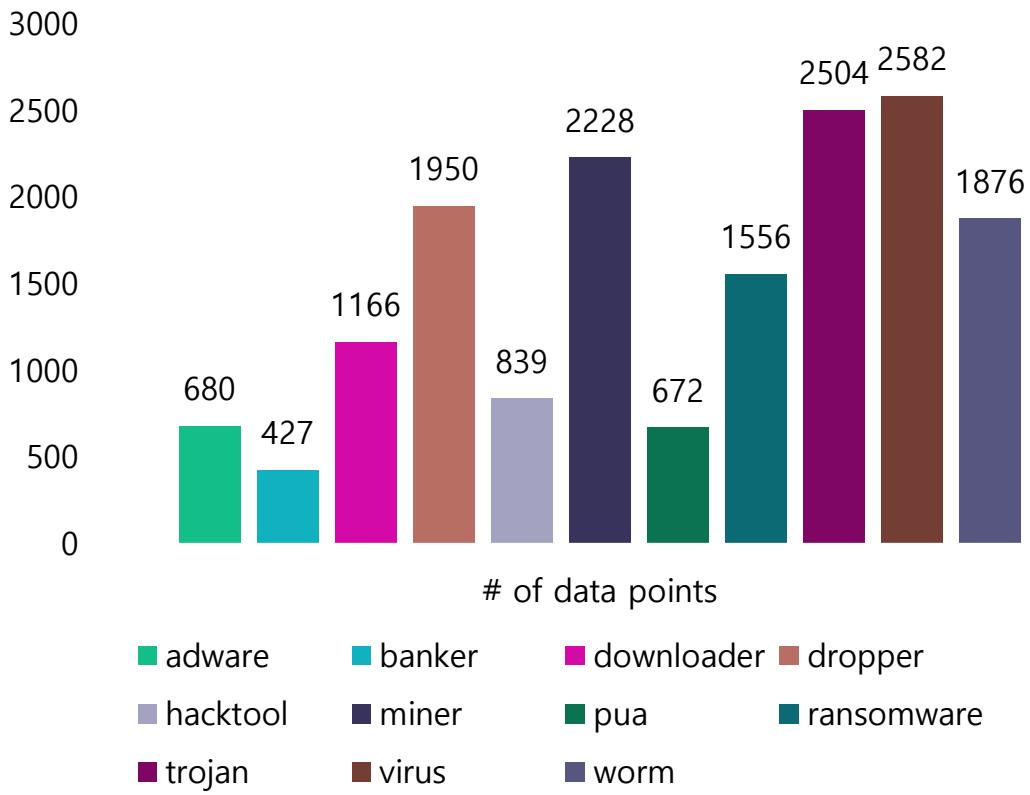
Malware Family Classification



Malware Family Classification



Malware Family Classification



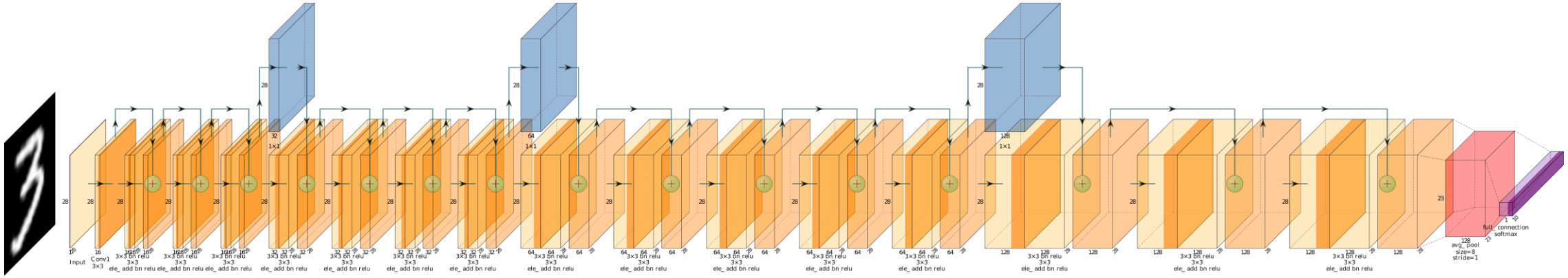
We performed over-sampling with `imblearn.over_sampling.`**`RandomOverSampler`**

Object to over-sample the minority class(es) by picking samples at random with replacement.

The bootstrap can be generated in a smoothed manner.

Malware Family Classification

ResNet50



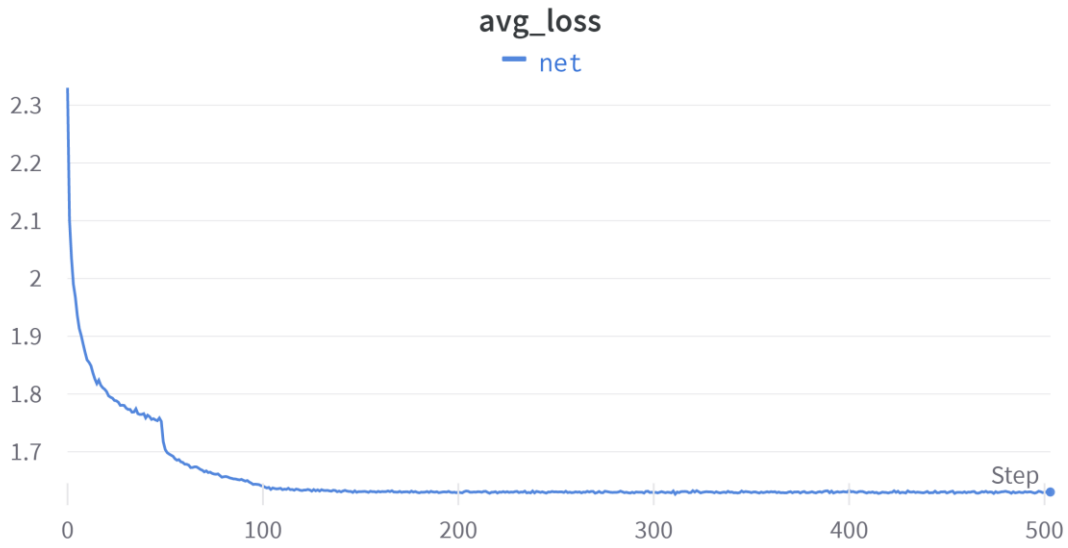
Which malware family does this virus belong to?

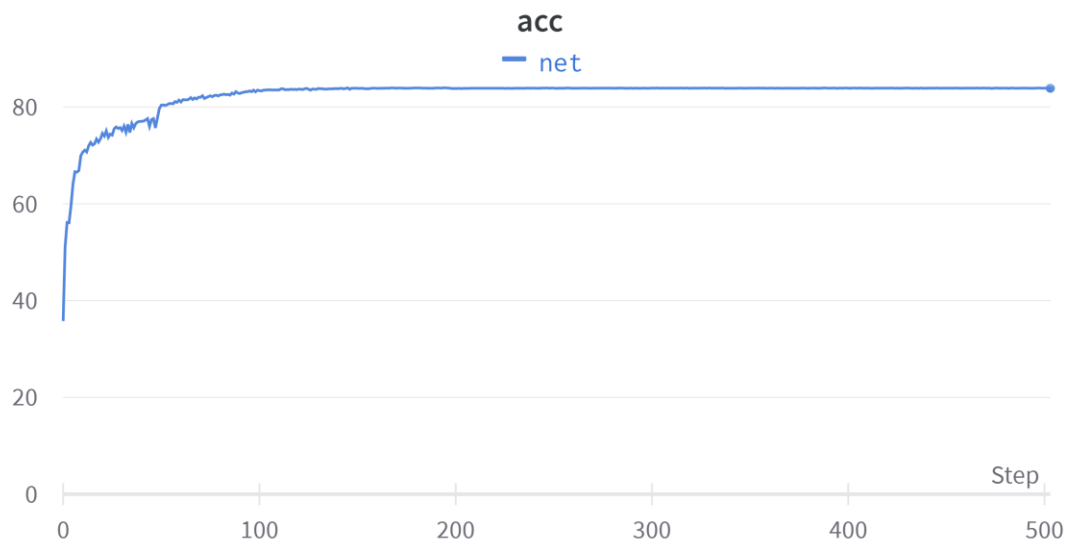
multi-class classification

```
self.resnet_50.fc = nn.Sequential(
    nn.Linear(2048, 1000),
    nn.ReLU(inplace=True),
    nn.Linear(1000, 256),
    nn.ReLU(inplace=True),
    nn.Linear(256, 64),
    nn.ReLU(inplace=True),
    nn.Linear(64, 11),
    nn.Softmax()
)
```

Malware Family Classification

Performance



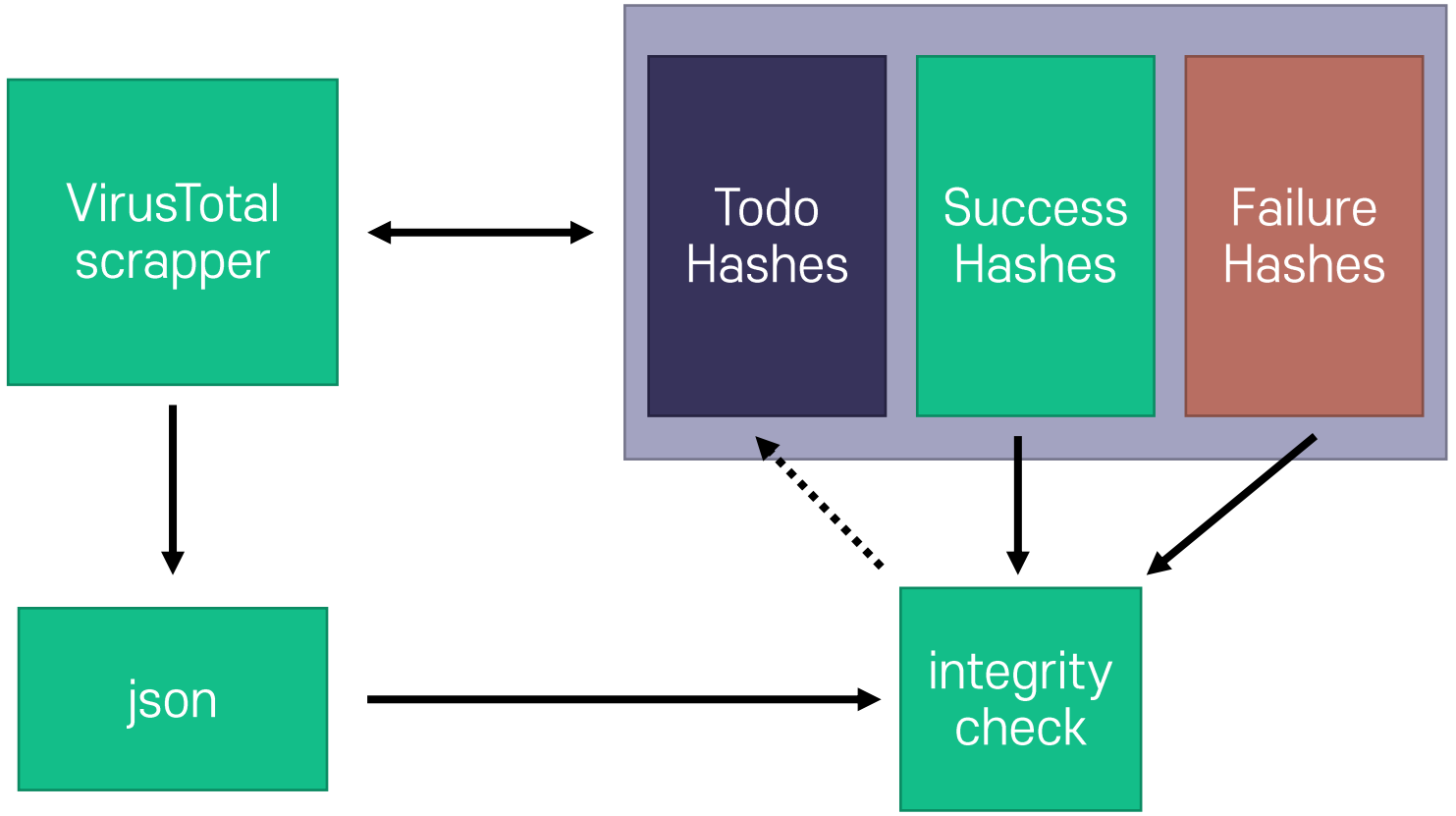


test set accuracy: 84%

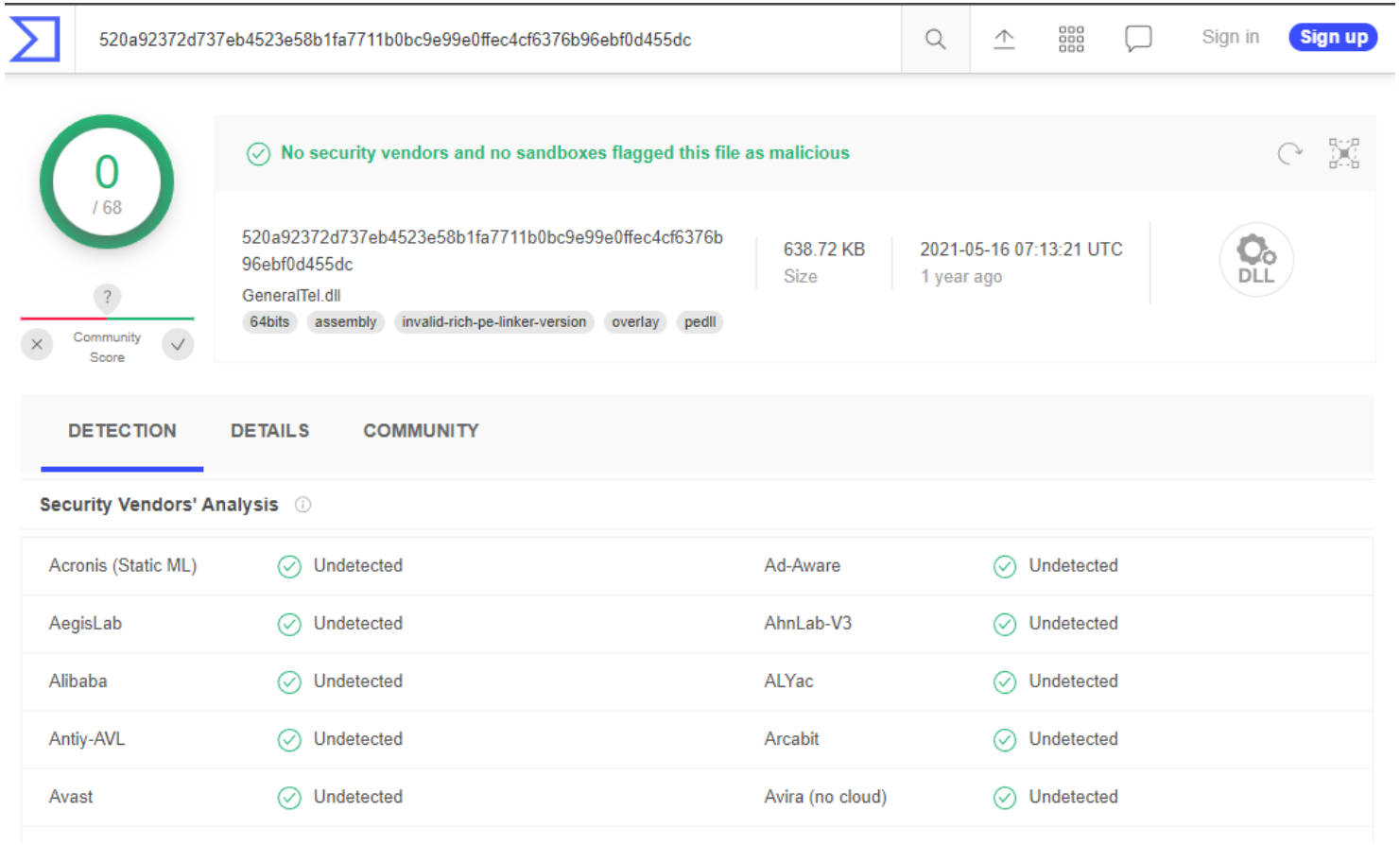
Other works

Analysis of malware feature importance

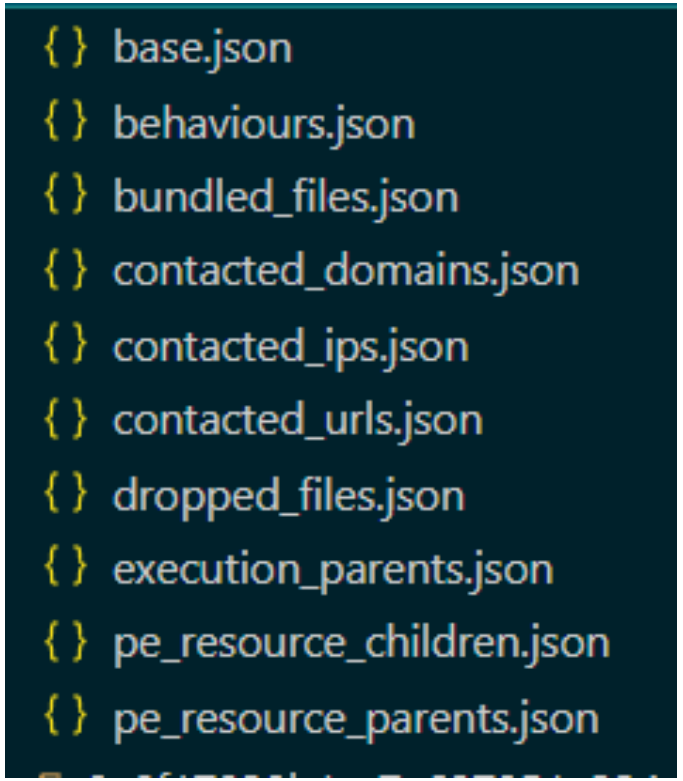
Malware Binary Classification



Malware Binary Classification



- Folder: 40,000
- Files: 414,784
- Capacity: 2.84GB



Malware Binary Classification

Type description

- Win32 DLL
- Win32 EXE
- JavaScript
- …

TrID

- Win32 Executable MS Visual C++ (generic)
- OS/2 Executable (generic)
- Microsoft Visual C++ compiled executable (generic)
- …

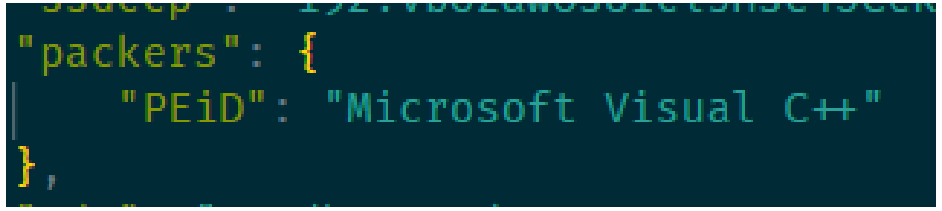
Malware Binary Classification


```
"popular_threat_classification": {
    "suggested_threat_label": "trojan.stormattack/ddos",
    "popular_threat_category": [
        {
            "count": 28,
            "value": "trojan"
        },
        {
            "count": 7,
            "value": "dropper"
        }
    ],
    "popular_threat_name": [
        {
            "count": 12,
            "value": "stormattack"
        },
        {
            "count": 8,
            "value": "ddos"
        },
        {
            "count": 7,
            "value": "rincux"
        }
    ]
},
```


Popular threat category/name

- Trojan
- Worm
- Virus
- Dropper
- DDOS
- ...

Malware Binary Classification



Packers

- PEiD
  - UPX
  - Microsoft Visual C++ v6.0 DLL
  - .NET executable
  - ...

Malware Binary Classification


```
"overlay": {
    "entropy": 2.0,
    "offset": 61440,
    "chi2": 252.0,
    "filetype": "ASCII text",
    "md5": "2f5f7485fd0c9653a9338251cad59e8b",
    "size": 4
},
"entry_point": 9844,
"machine_type": 332,
"imphash": "ba23a556ac1d6444f7f76feafd6c8867",
"sections": [
    {
        "virtual_size": 6298,
        "entropy": 5.13,
        "name": ".text",
        "raw_size": 8192,
        "virtual_address": 4096,
        "md5": "6dfbc6899241990b3bc003eef552e520"
    },
    {
        "virtual_size": 2712,
        "entropy": 4.11,
        "name": ".rdata",
        "raw_size": 4096,
        "virtual_address": 12288,
        "md5": "29aa83f4db54de6e04f0b3f5c0e545df"
    },
```


Sections

- Overlay
  - Entropy
  - Chi2
  - …
- .text, .rdata, .rsrc …
  - Entropy

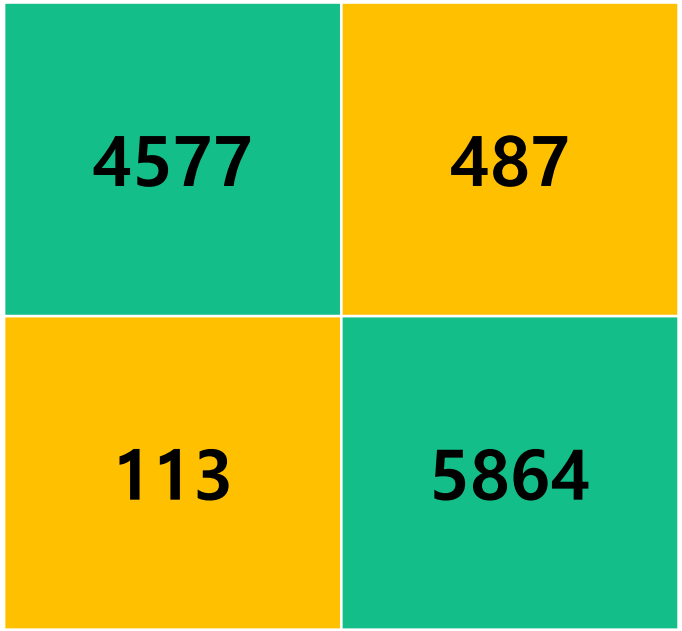
Malware Binary Classification

type_des	best_trid_	best_trid_	type_exte	has_signa	packer	type_tag	overlay_e	overlay_c	overlay_fi	dropped_	beha
Win32 DL	Win32 Exe	33.7	dll	0	unknown	pedll	2	252	ASCII text	0	
Win32 DL	Win64 Exe	61.7	dll	0	unknown	pedll	2	252	ASCII text	0	
Win32 EX	OS/2 Exec	25.2	exe	1	unknown	peexe	0.004528	2.58E+09	Data	0	
Win32 DL	Windows	83.7	dll	1	unknown	pedll	7.398872	22471.63	Data	0	
Win32 EX	Win32 Exe	42.7	exe	0	unknown	peexe	2	252	ASCII text	0	
Win32 DL	Win32 Exe	33.7	dll	1	Microsoft	pedll	2	252	ASCII text	0	
Win32 DL	Win32 EX	60.7	dll	0	UPX	pedll	2	252	ASCII text	0	
Win32 EX	Microsoft	33.5	exe	0	unknown	peexe	2	252	ASCII text	0	
Win32 EX	Win32 Exe	41	exe	0	Microsoft	peexe	4.818212	96692040	Data	0	
Win32 EX	Win32 Exe	58.7	exe	1	Microsoft	peexe	7.406668	7600.766	Data	0	
Win32 DL	Win64 Exe	82	dll	0	unknown	pedll	1.212236	52465.13	ASCII text	0	
Win32 EX	Win64 Exe	42.3	exe	1	UPX v0.89	peexe	3.649286	5206.675	Data	0	
Win32 EX	Win64 Exe	82	exe	1	unknown	peexe	7.999897	268.3149	Data	0	
Win32 DL	Generic_M	65.9	dll	1	Microsoft	pedll	2	252	ASCII text	0	

hash
type_description
best_trid_type
best_trid_probability
type_extension
has_signature
packer type_tag
overlay_entropy
overlay_chi2
overlay_filetype
dropped_files_count
behaviours_count
contacted_domains_count
contacted_ips_count
contacted_urls_count
.text_entropy .bss_entropy .rdata_entropy .data_entropy
.xdata_entropy .idata_entropy .pdata_entropy
.rsrc_entropy .reloc_entropy .CRT_entropy

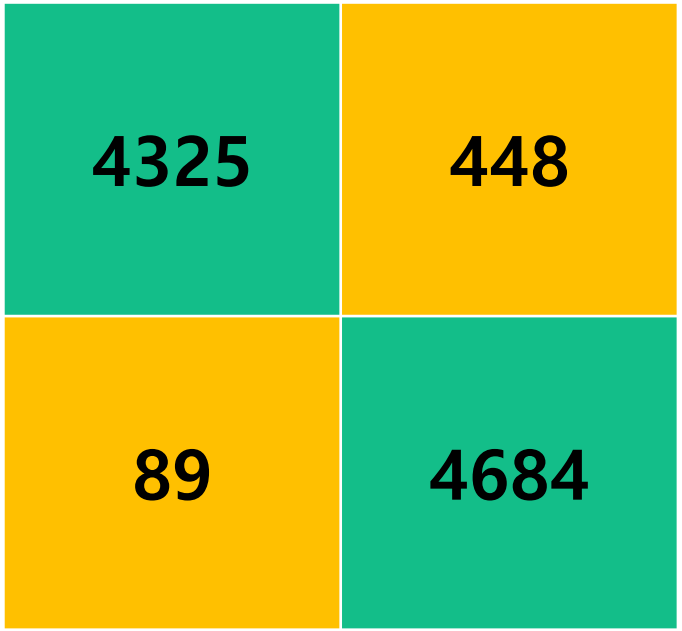
Malware Binary Classification

Test set 1



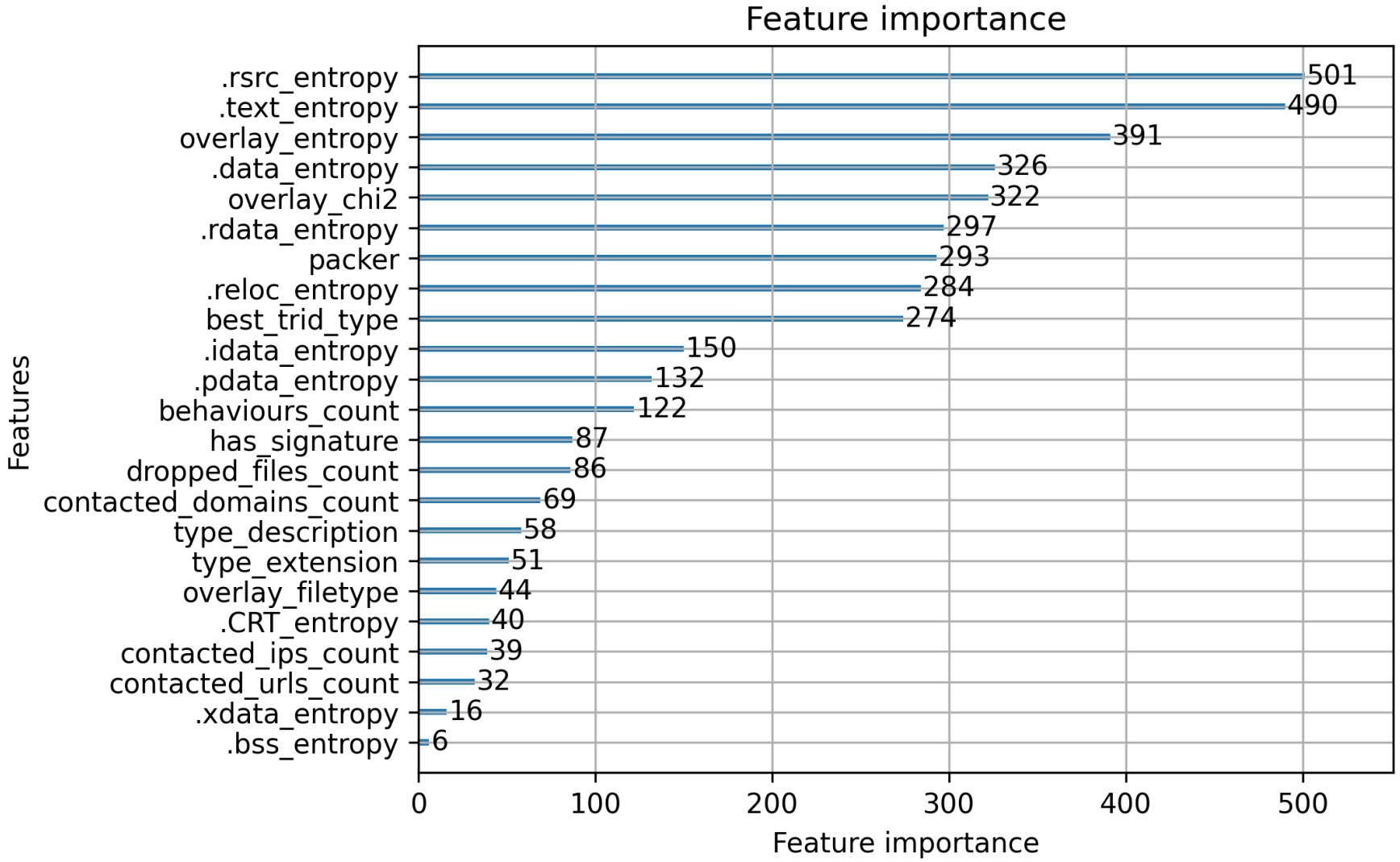
Accuracy: 96.15%
Precision: 93.99%

Test set 2



Accuracy: 94.37%
Precision: 91.27%

Malware Binary Classification



Thank You ☺

Hyeonsu Kim, Gaon Choi.

Department of Computer Science

Hanyang University