

Black Hat Europe 2019 Arsenal



AVCLASS++ Yet Another Massive Malware Labeling Tool

NTT Secure Platform Laboratories

Yuma Kurogome




Machine Learning



- Gold rush
 - Malware detection, classification, attribution, ...
- Supervised learning
 - **Labeled** training data is needed
- Unsupervised learning
 - **Labeled** data is needed, for evaluation, after all

Label	Sepal length	Sepal width	Petal length	Petal width
Setosa	5.1	3.5	1.4	0.2
Setosa	4.9	3.0	1.4	0.2
Versicolor	6.4	3.5	4.5	1.2
...				

Labeling Problem

- Manual labeling may not scale
 -    ...
- VirusTotal (VT) comes to rescue
 - Input:
 - Malware sample
 - Output
 - Antivirus (AV) scan results
- Problem
 - Sometimes AVs return different names
 - Which AV do you trust?
 - How to aggregate multiple AV scan results to one label?



49
/ 66

Community Score

49 engines detected this file

df6a06f533def5dc2590c0e3cbe8dc9e9b52e0be891fe5491fc31b5143a750822
bilonebilo202.exe

156.00 KB
Size

2018-10-27 01:06:22 UTC
1 year ago

Details

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Trojan.GenericKD.12516581		AhnLab-V3	Trojan/Win32.Lebag.R211231
Antiy-AVL	Trojan/Win32.TSGeneric		Arcabit	Trojan.Generic.DBEFCES
Avast	Win32:Malware-gen		AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1018121		BitDefender	Trojan.GenericKD.12516581
CAT-QuickHeal	Trojan.IGENERIC		ClamAV	Win.Trojan.Emotet-6357146-0
CrowdStrike Falcon	Malicious_confidence_100% (W)		Cybereason	Malicious.acbf66
Cylance	Unsafe		Cyren	W32/Locky.CY.genEldorado
DrWeb	Win32.HLLM.Reset.493		Emsisoft	Trojan.GenericKD.12516581 (8)
Endgame	Malicious (high Confidence)		eScan	Trojan.GenericKD.12516581
ESET-NOD32	A Variant Of Win32/Kryptik.FYGP		F-Prot	W32/Locky.CY.genEldorado
F-Secure	Trojan.GenericKD.12516581		Fortinet	W32/Kryptik.FXW.Mtr
GData	Trojan.GenericKD.12516581		Ikarus	Trojan.Win32.Tofee
K7AntiVirus	Trojan (0051ab21)		K7GW	Trojan (0051a6501)



- Malware labeling tool
 - Aggregates AV scan results and output label(s)
 - Input:
 - VT report(s)
 - Malware sample(s) (optional)
 - Output:
 - Label(s)
- Based on AVCLASS
 - One of the most well-used oracles in such a scenario

AVCLASS: A Tool for Massive Malware Labeling

[M Sebastián](#), [R Rivera](#), [P Kotzias](#)... - ... Symposium on Research ..., 2016 - Springer

Labeling a malicious executable as a variant of a known family is important for security applications such as triage, lineage, and for building reference datasets in turn used for evaluating malware clustering and training malware classification approaches. Oftentimes ...

☆  [Cited by 137](#) [Related articles](#) [All 6 versions](#)

Features

- Automatic
 - AVCLASS++ removes manual analysis limitations on the size of the input dataset
- Vendor-agnostic
 - AVCLASS++ operates on the labels of any available set of AV engines, which can vary from sample to sample
- Cross-platform
 - AVCLASS++ can be used for any platforms supported by AV engines, e.g., Windows or Android malware



Features



- Does not require executables
 - AV labels can be obtained from online services like VT using a sample's hash, even when the executable is not available
 - Yet, AVCLASS++ has also a potential that can improve label accuracy if there are executables
- Quantified accuracy
 - The original AVCLASS had evaluated on five publicly available malware datasets with ground truth
 - AVCLASS++ is further tuned to perform under adverse conditions
- Open source
 - Check out the QR code!

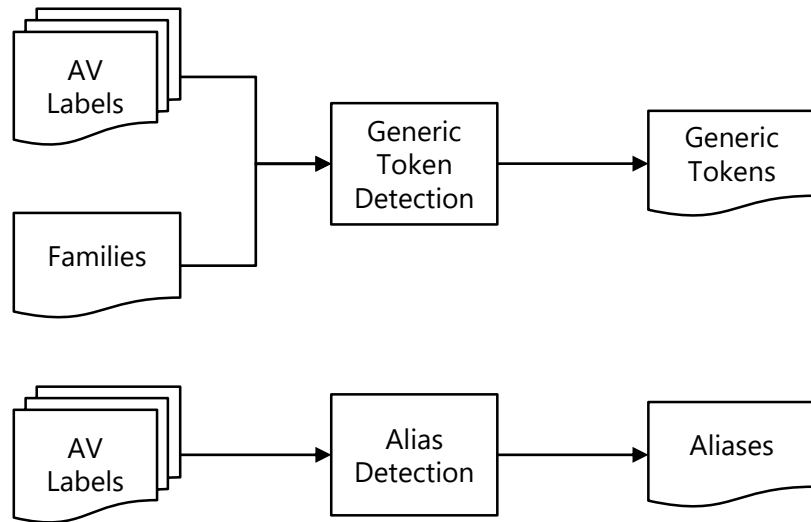
Workflow

- AVCLASS++ has three phases:
 - Preparation
 - Labeling
 - Label Propagation



Preparation (Optional)

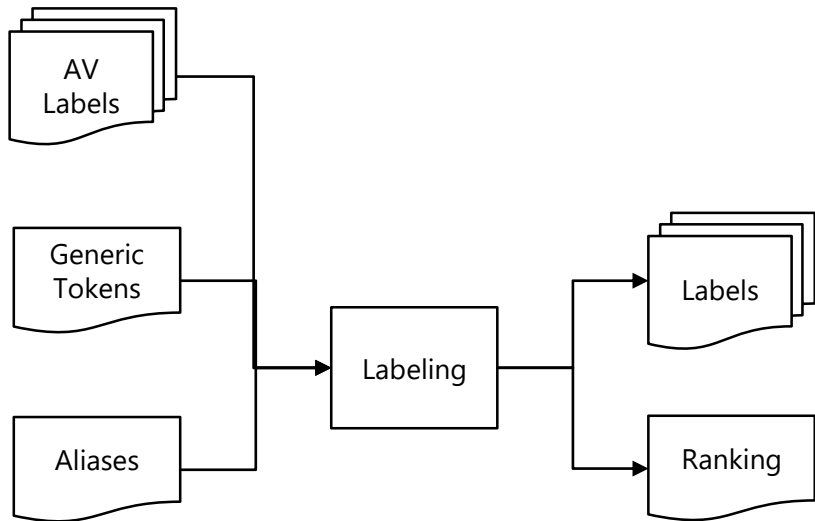
- AVCLASS++ requires the two files other than VT reports
 - Generic tokens
 - Aliases
- AVCLASS++ shipped with the pre-configured files
 - You don't need to touch them
 - But you can customize them



Labeling



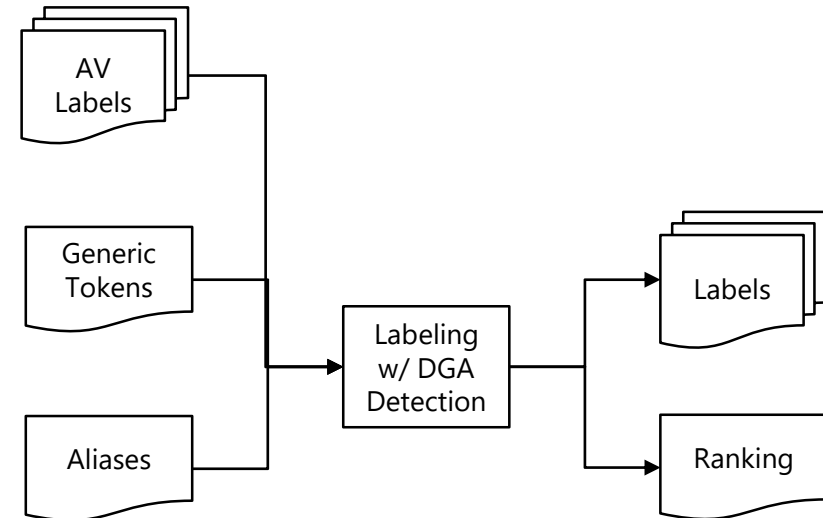
- AVCLASS++ generates malware label(s) as follows:
 - For each scan result:
 - Remove suffixes
 - Win32/pony.c → Win32/pony
 - Filter unnecessary tokens
 - Win32/pony → pony
 - Replace aliases
 - pony → fareit
 - After that, AVCLASS++ creates a ranking
 - The most popular label would be output
 - Also, a ranking itself can be output



Labeling – DGA Detection

- AVCLASS fails to labeling when:
 - Malware label name is randomly generated
- Domain generation algorithm (DGA)
 - Malware uses DGA to generates new domain names
 - Some AVs use DGA-like methods to generate malware label names
- Why not divert DGA detection methods to remove such a label?
 - Meaningful characters ratio
 - N-gram normality score

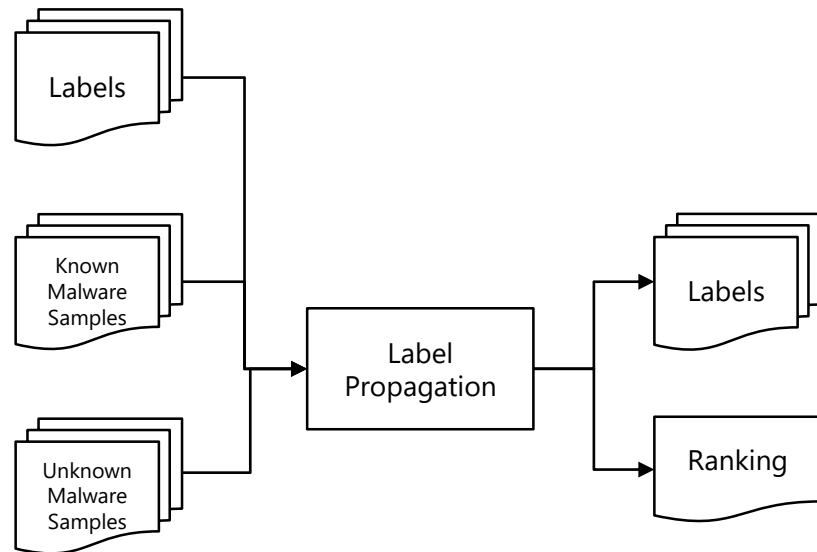
❗	Gen:Trojan.Heur.MmNfrHGm40bj1
❗	Trojan.Heur.MmNfrHGm40bj1
❗	Win32:Malware-gen
❗	Gen:Trojan.Heur.MmNfrHGm40bj1



Label Propagation (Optional)



- AVCLASS also fails to labeling when:
 - No AV signatures at VT submissions
 - Only generic signatures reacted
- AVCLASS++ finds labels for unlabeled samples by:
 - Extracting PE file features:
 - Headers
 - Sections
 - Imports
 - ...
 - Propagating labels from similar samples



AVCLASS vs AVCLASS++

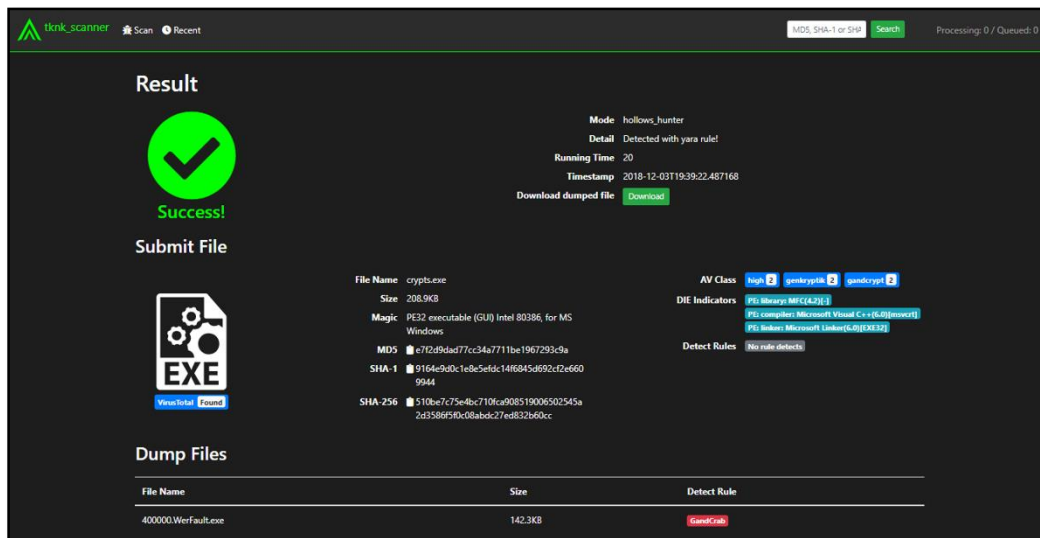


	AVCLASS	AVCLASS++
Labeling	✓	✓
Family Ranking	✓	✓
PUP Classification	✓	✓
Ground Truth Evaluation	✓	✓
Generic Token Detection	✓	✓
Alias Detection	✓	✓
DGA Detection		✓
Label Propagation		✓
Python 3 Compatible		✓

Showcase – nao-sec/tknk_scanner



- Automated malware analysis system
 - Integrated with VT, YARA, and hollows_hunter
 - Input:
 - Malware sample
 - YARA rules
 - Output:
 - Label
 - Memory dump
 - ...



The screenshot displays the tknk_scanner web interface. At the top, there's a navigation bar with 'tknk_scanner', 'Scan', and 'Recent' buttons, along with a search bar and a 'Processing: 0 / Queued: 0' status. The main section is titled 'Result' and features a large green checkmark icon with the text 'Success!'. Below this is a 'Submit File' button and a file icon labeled 'EXE'. The analysis details for 'crypts.exe' are shown, including its size (208.9KB), magic (PE32 executable (GUI) Intel 80386, for MS Windows), MD5, SHA-1, and SHA-256 hashes. The AV Class is 'High' with 'genscryptik' and 'jandcrypt' engines. The Detect Rules section shows 'No rule detected'. A 'Dump Files' table at the bottom lists a file named '400000.WerFault.exe' with a size of '142.3KB' and a 'Detect Rule' of 'Genscriptik'.

File Name	Size	Detect Rule
400000.WerFault.exe	142.3KB	Genscriptik



DEMO

