CZNIC HaaS Malware Analysis

CyberSecurity Technology Institute,
Institute for Information Industry

Presenter : Chia Min, Sena, Lai

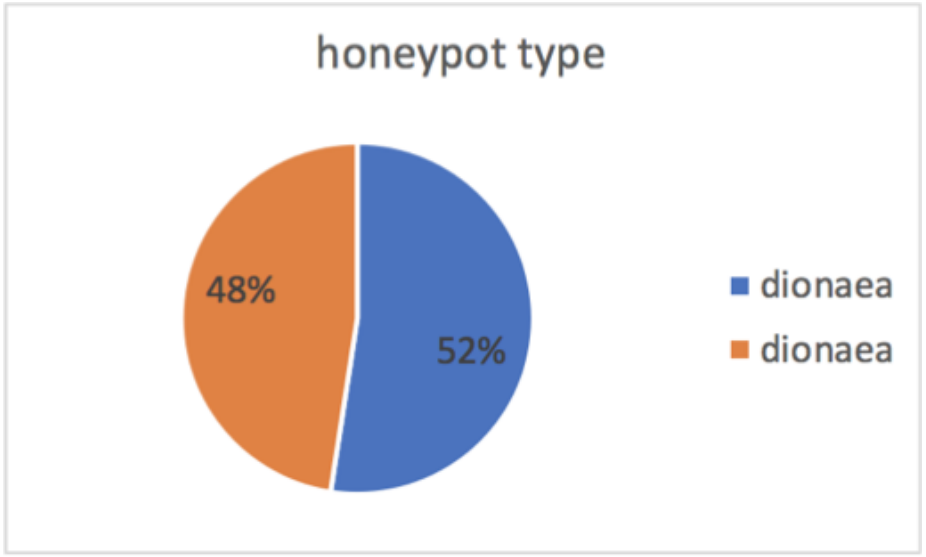
Outline

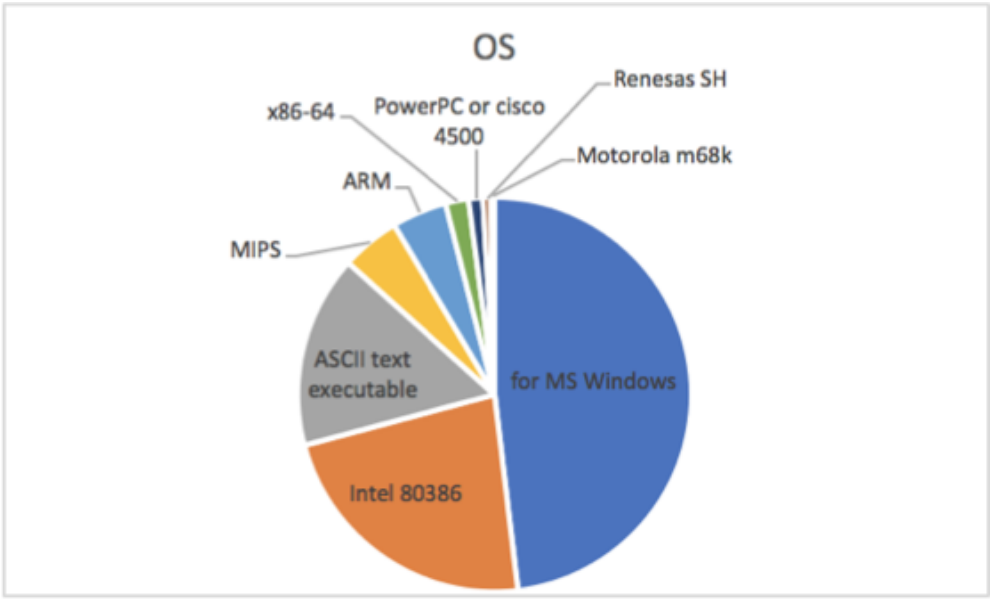
- The Cooperation of CZ.NIC and III
- Statistics Result of Malware
- Malware Family Classiffication
- Malicious Domain Analysis

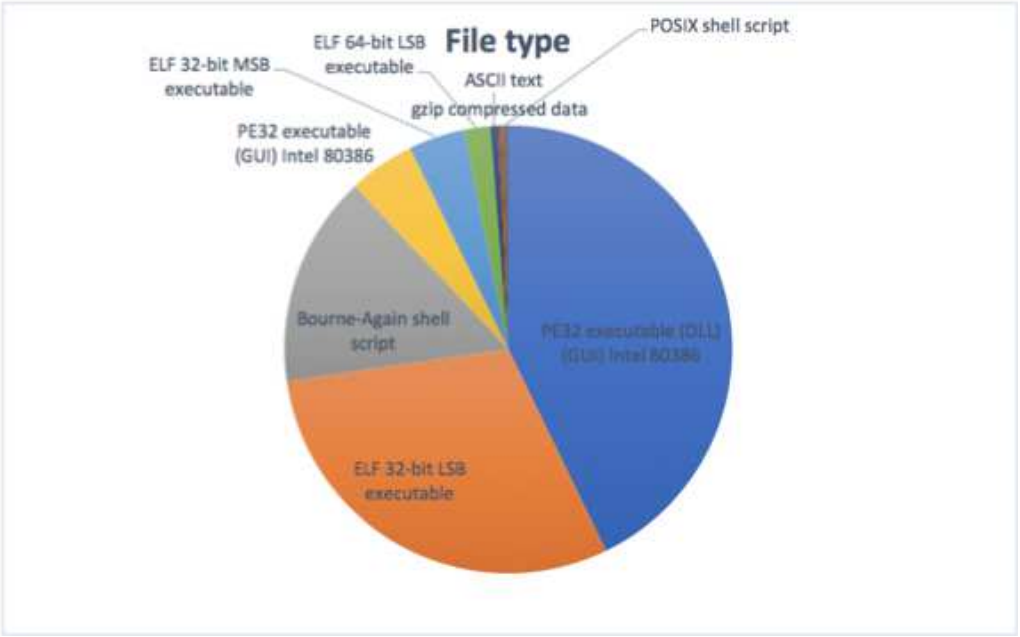
The Cooperation of CZ.NIC and III

- Implement HaaS Project from 1. June 2016 to 31. May 2018
- CZ.NIC provides malware samples to III
  - Dionaea: 6071 (~ 13. Feb. 2018)
  - Cowrie: 8220 (~ 13. Feb. 2018)

Statistics







Hard coded IP

IP	Count	Information
192.168.1.101	383	Private
62.4.24.135	32	French
62.4.24.135 163.172.18.61 8.8.8.8	27	French UK USA google DNS

Map the category with VT information

- Extract Indicators of Compromise (IoC) from malware samples and obtain more information through VirusTotal (VT)

[ref] **https://www.virustotal.com/#/home/upload**

virustotal

SHA256:

File name: Bins.sh

Detection rate: 22 / 56

Analysis date: 2017-05-18 02:10:30 UTC (October, 1 week ago)

analysis | Other information | Comment 1 | vote

File identification

MD5	
SHA1	
SHA256	
Ssdeep	24: vcyEorpMvPWHs4rlHNUGA/dWJa3Smu3eTsm:vdEorq+M4rONUGGdUa3C6R
File size	1.6 KB (1600 bytes)
File type	unknown
Magic literal	Bourne-Again shell script text executable
TrID	Linux/UNIX shell script (100.0%)

VirusTotal metadata

First submission	2017-04-22 04:42:53 UTC (November, 1 week ago)
Last submission	2017-04-22 04:42:53 UTC (November, 1 week ago)

virustotal

SHA256:

File name: Bins.sh

Detection rate: 22 / 56

Analysis date: 2017-05-18 02:10:30 UTC (October, 1 week ago)

analysis | Other information | Comment 1 | vote

Antivirus	result	Updated
Ad-Aware	Trojan.Downloader.BashAgent.TX	20170518
AegisLab	Troj.Downloader.Shell!c	20170518
ALYac	Trojan.Downloader.BashAgent.TX	20170518
Arcabit	Trojan.Downloader.BashAgent.TX	20170518
Avast	BV:Downloader-IB [Drp]	20170518
AVG	Linux/Downloader.CP	20170518
BitDefender	Trojan.Downloader.BashAgent.TX	20170517
Cyren	Trojan.MAQB-3	20170518
DrWeb	Linux.DownLoader.275	20170518

However...

virustotal

SHA256:

File name: Index.html

Detection rate: 0 / 56

Analysis date: 2018-01-24 09:36:59 UTC (2 months ago)

analysis | Other information | Comment 1 | vote

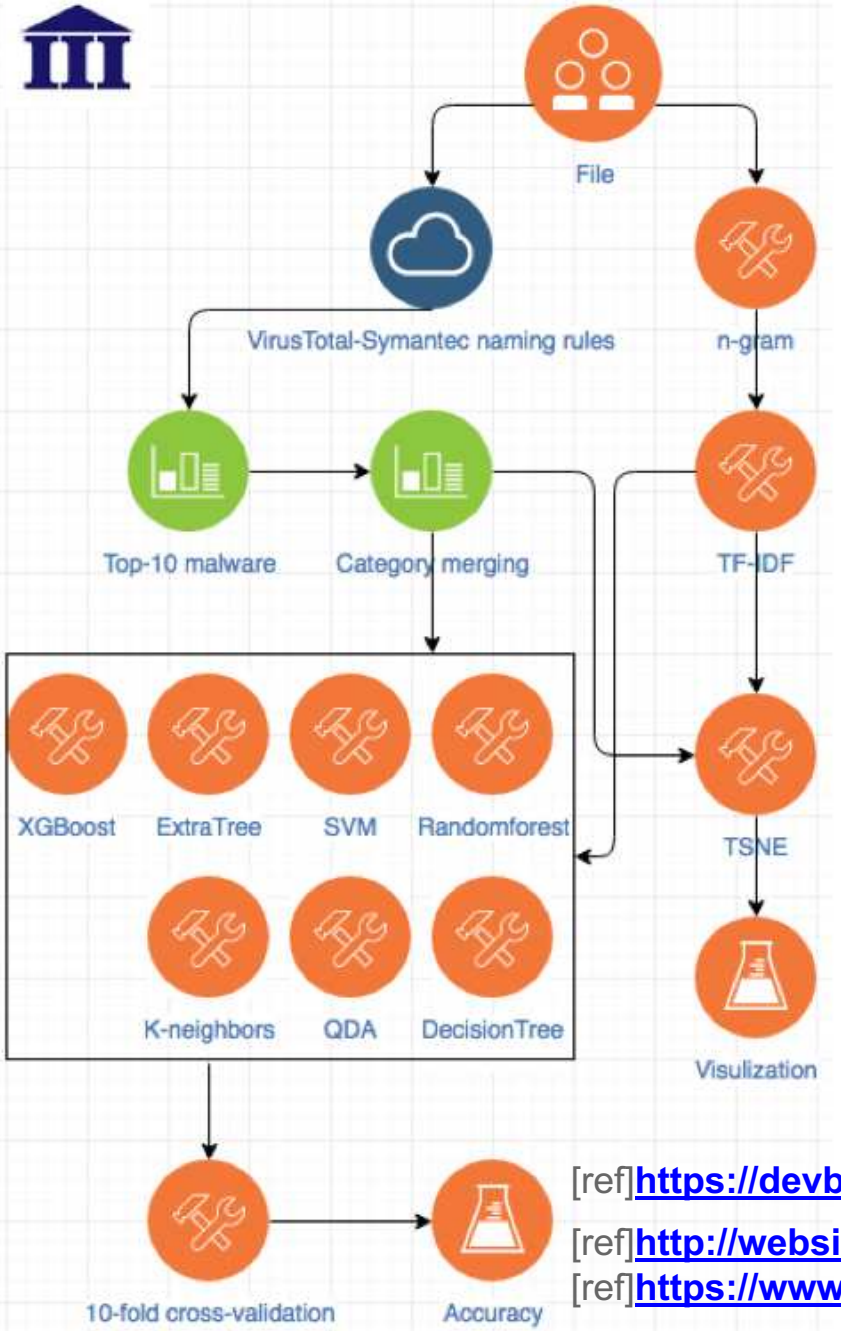
File identification

MD5	
SHA1	
SHA256	
Ssdeep	48: nSZLa5BNWvomYV8KYbgnrerxPerorq0QkIMxPzlSmX8mEtHmczmlhUE5soXXnRtl: MLYBNyXKYYrerxPerorq0hFxLlSmX8mz
File size	2.9 KB (3001 bytes)
File type	HTML
Magic literal	HTML document text
TrID	HyperText Markup Language with DOCTYPE (80.6%) HyperText Markup Language (19.3%)
Tags	Html

VirusTotal metadata

First submission	2018-01-24 09:36:59 UTC (2 months ago)
Last submission	2018-01-24 09:36:59 UTC (2 months ago)
File name	Index.html

Malware Families Classifier



Malware Family Classification

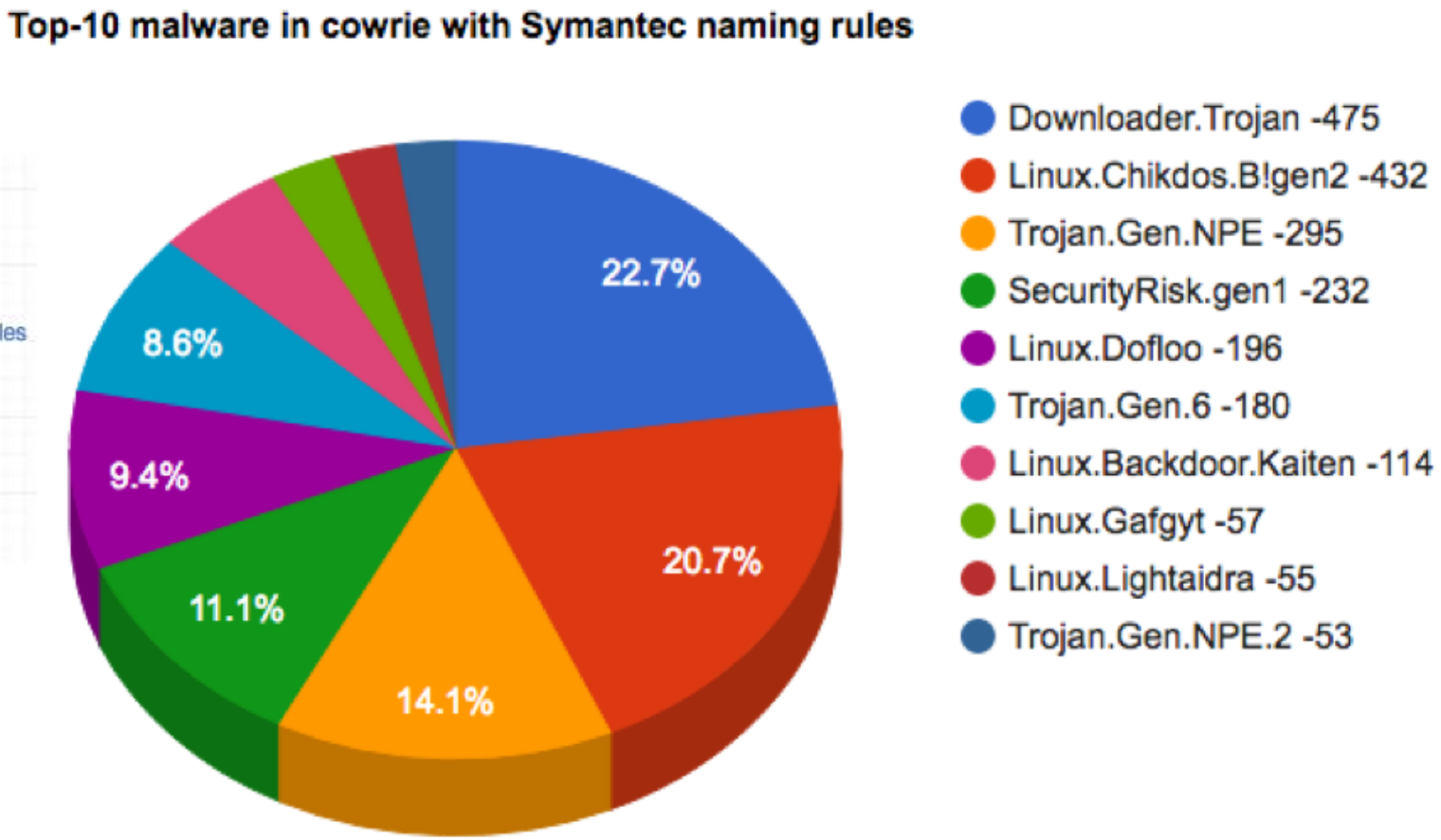
- Extract n-gram of binary bytes and transform them to computed features via TF-IDF.
- Adapt Symantec naming rules as malware families label.
- Show roughly malware families distribution in the way of projection by TSNE
- Find out which classification methods can get best performance of accuracy rate.

[ref]https://devblogs.nvidia.com/malware-detection-neural-networks/

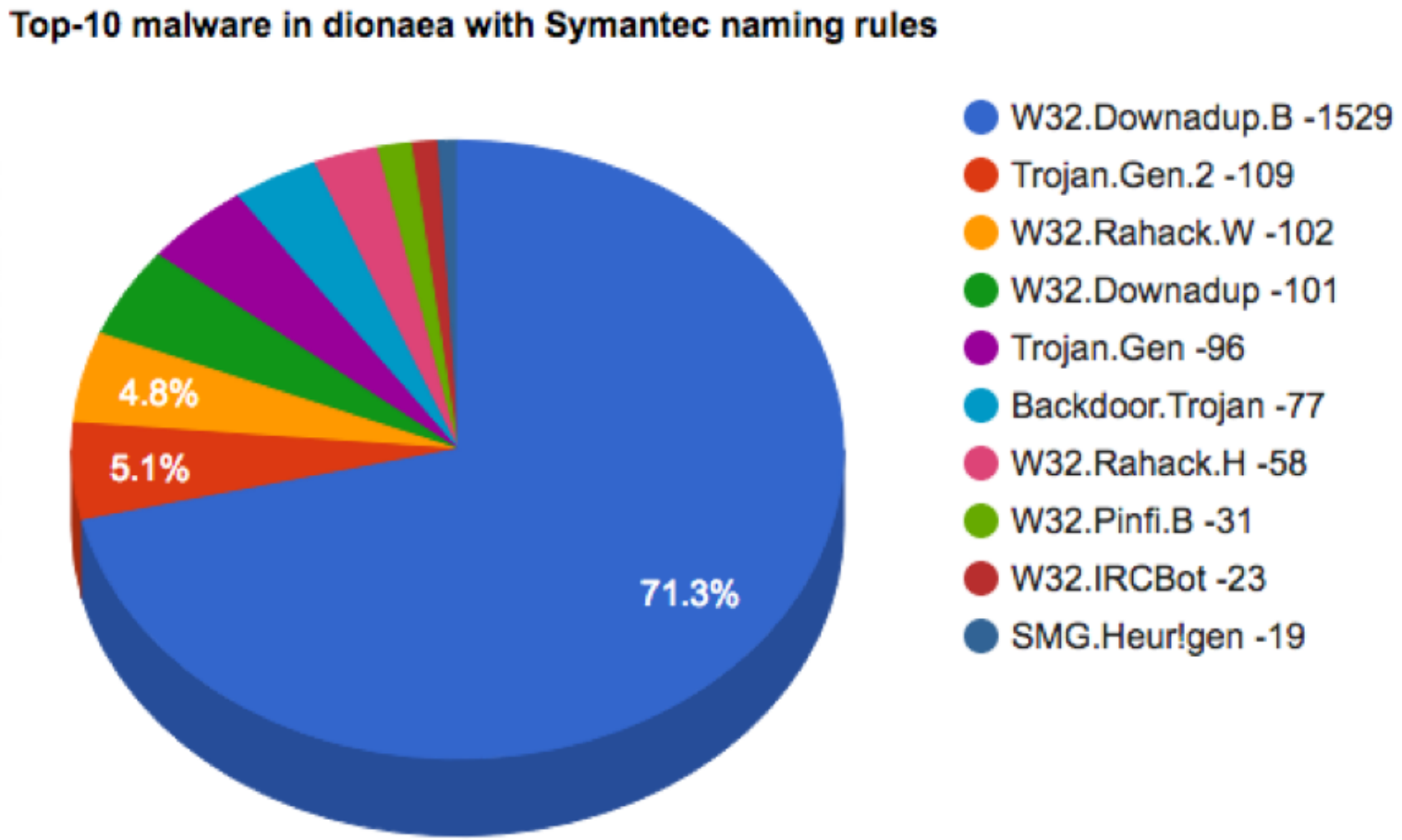
[ref]http://website.aub.edu.lb/fas/cs/grad_proj/Documents/posters16_17/Project2.pdf

[ref]https://www.symantec.com/security-center/virusnaming

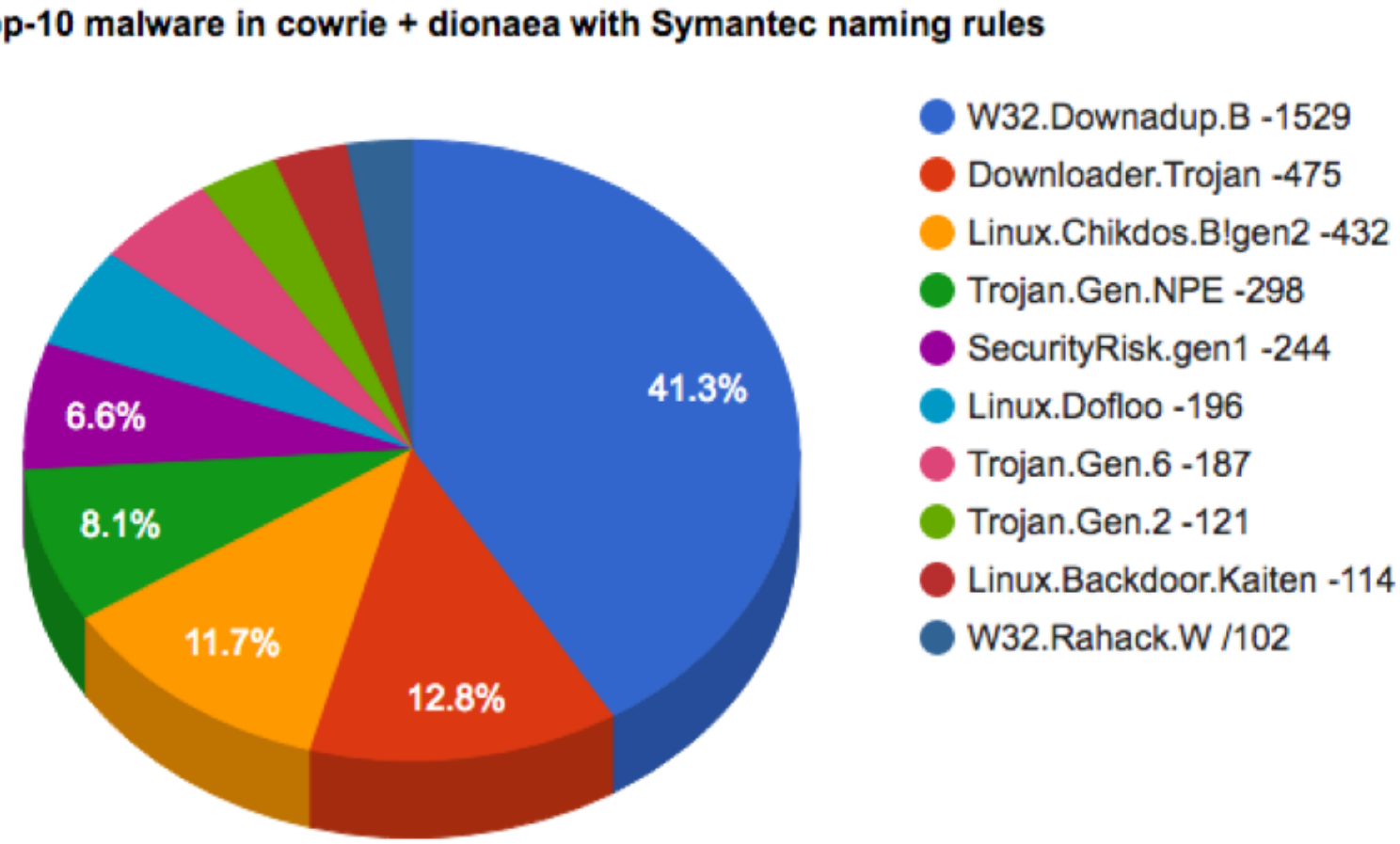
Get malware labels from VT



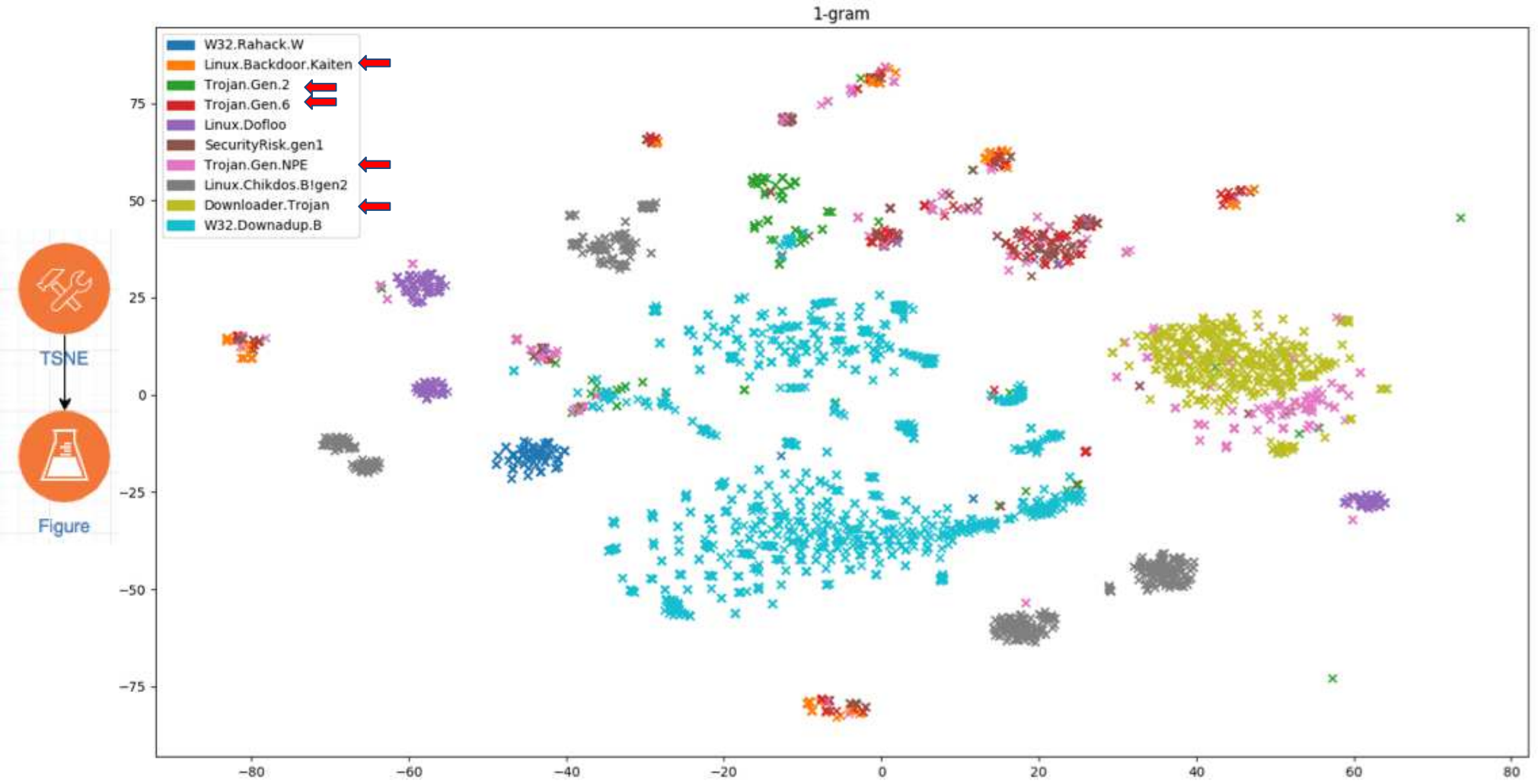
Get malware labels from VT



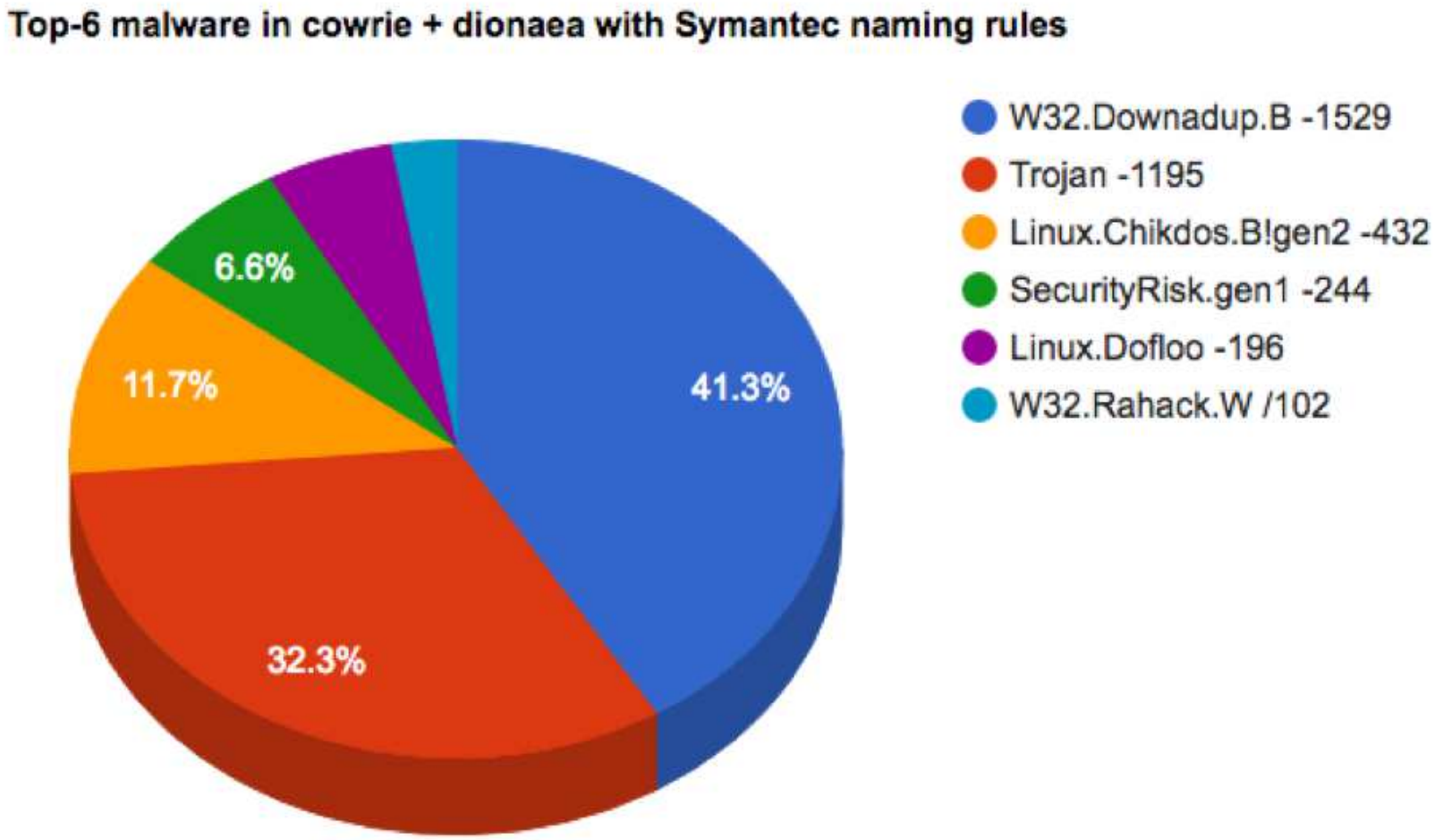
Get malware labels from VT



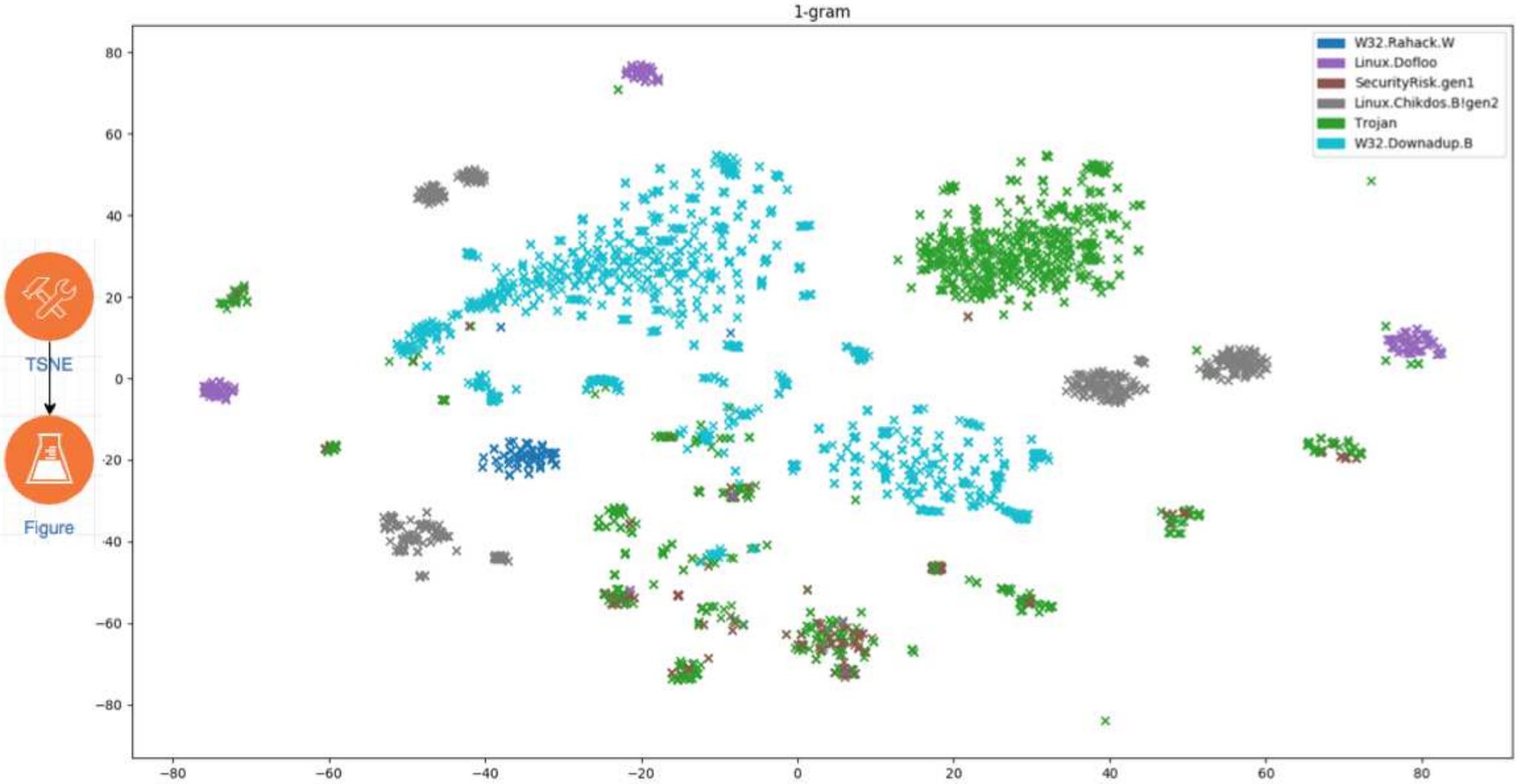
TSNE with 1-gram TF-IDF model



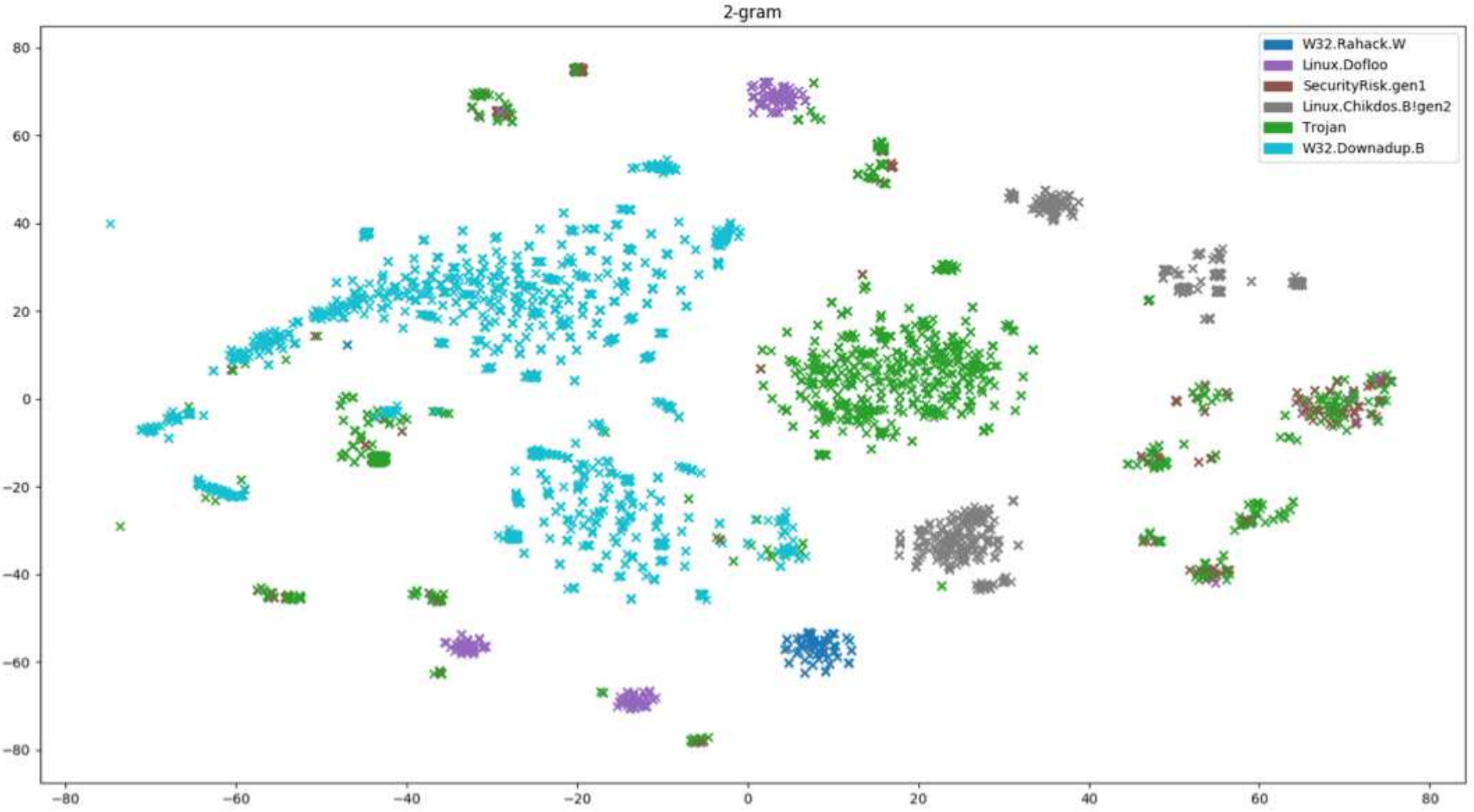
Category merging-
Merge to 6 malware



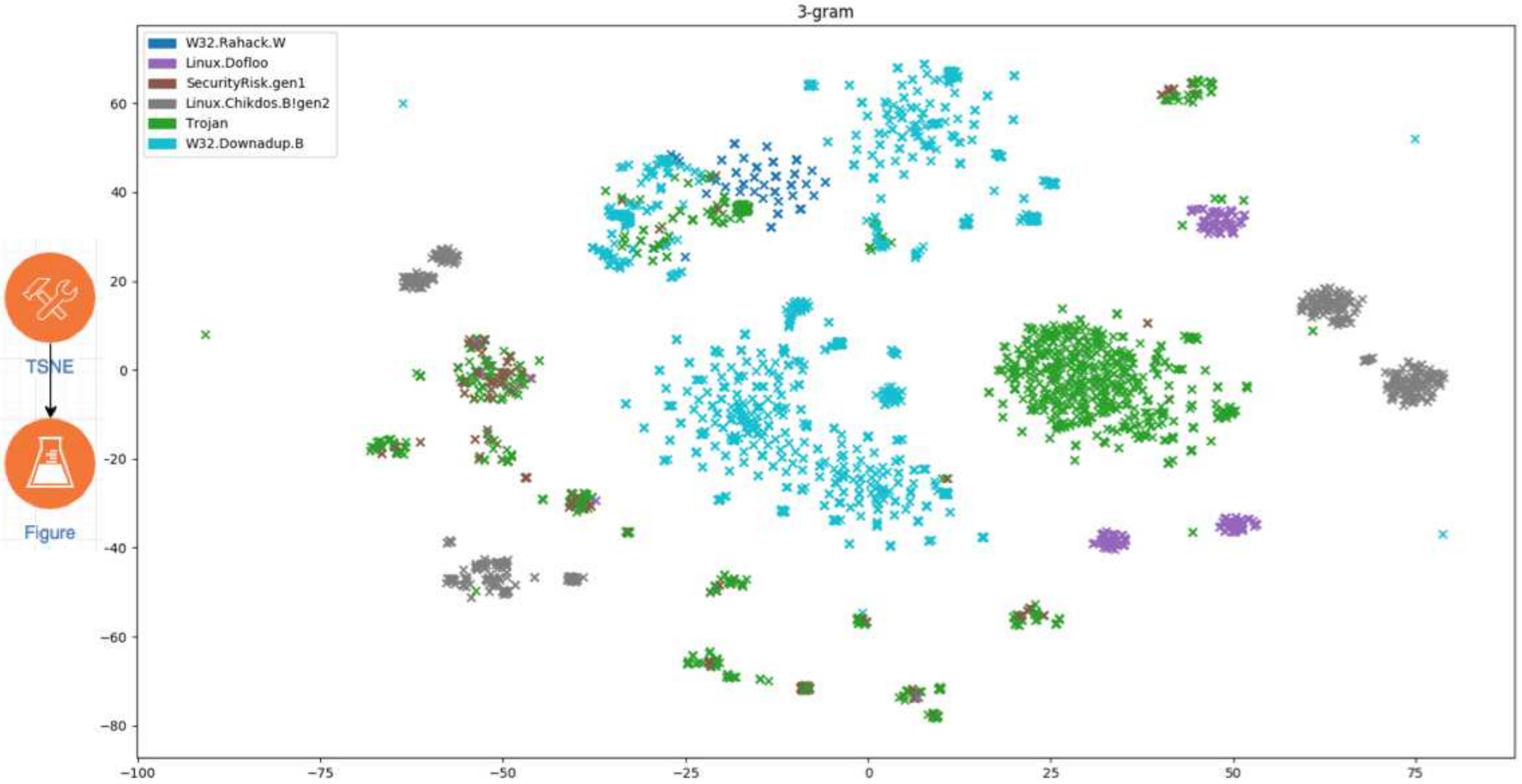
TSNE with 1-gram TF-IDF model



TSNE with 2-gram TF-IDF model



TSNE with 3-gram TF-IDF model



Classifiers comparison

N-grams comparison (accuracy)

About the Classifier

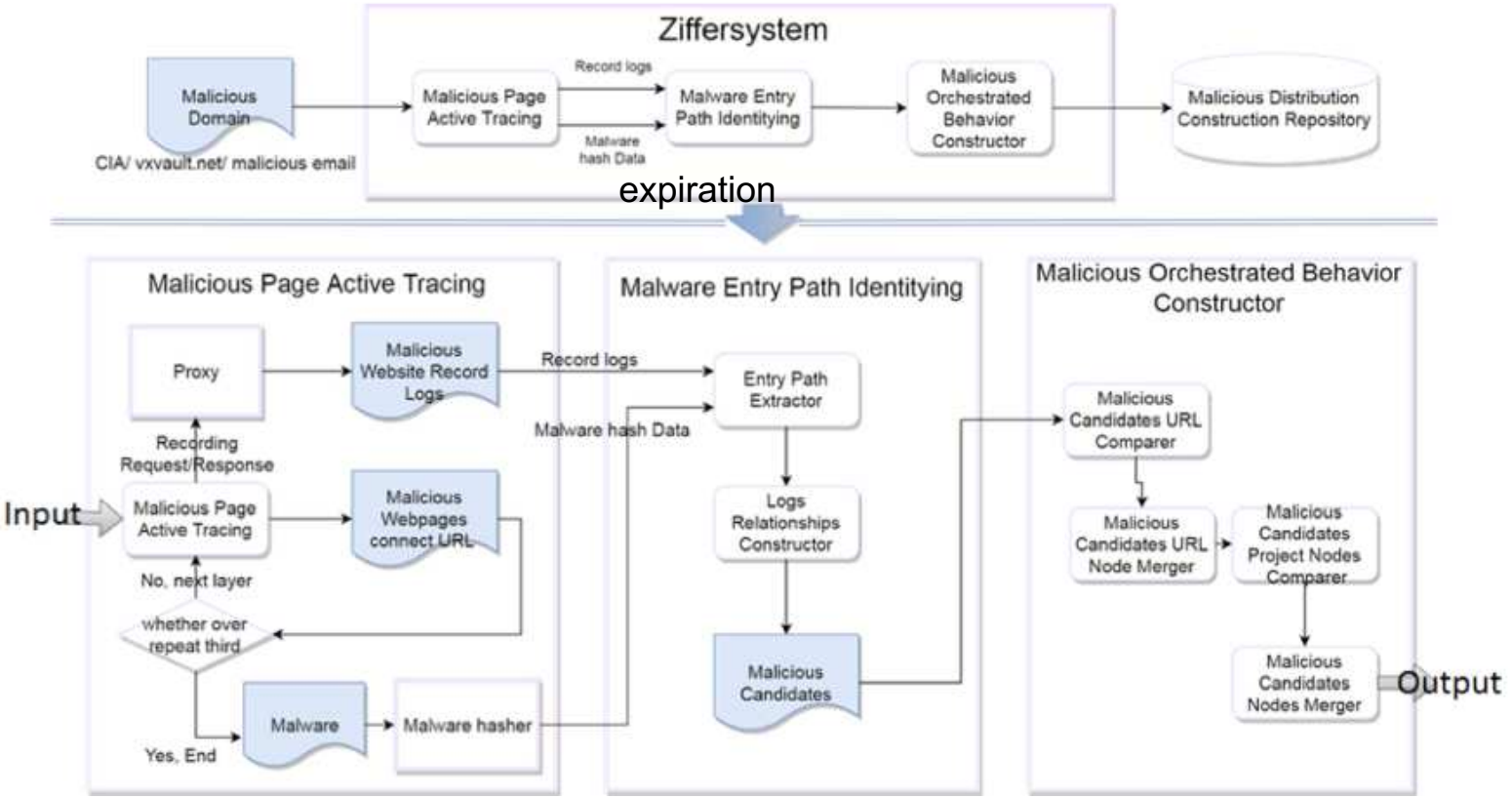
- Using only binary bytes information can help to distinguish different types of malware.
- Based on the features of 1-gram from binaries, we can classify malwares to their belonging families with high accuracy. The detection rate is over 95%.
- We can classify the unknown malwares into their belonging families.

Malicious Domain Analysis (1/3)

- Step 1: Run dynamic analysis for each malware sample.
- Step 2: Extract the URL list from network traffic logs
- Step 3: Extend the C2 via Ziffer system and get further understanding about each URL.

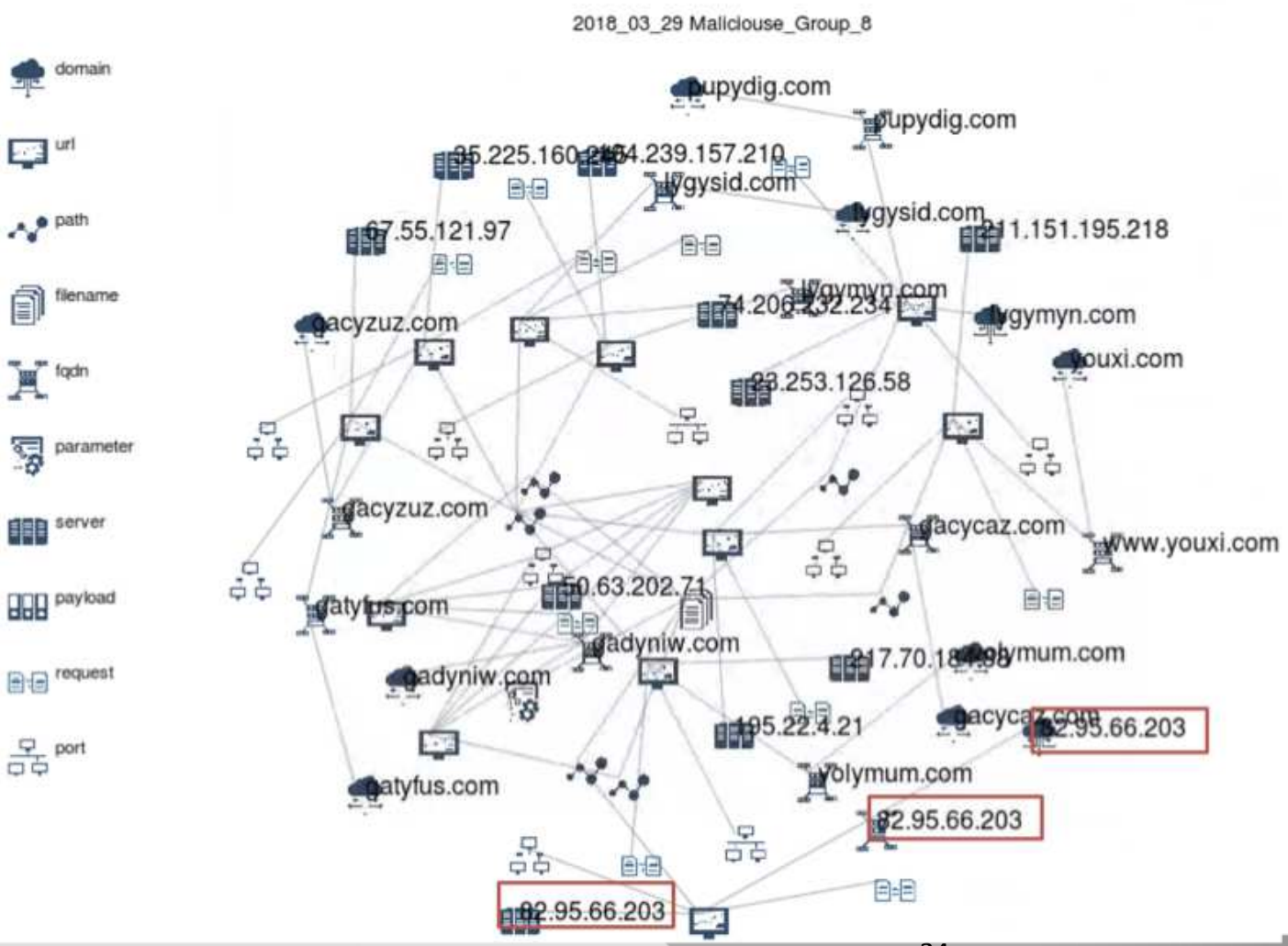
Malicious Domain Analysis (2/3)

- Explore Malware Distribution of each malicious domain name. The ZifferSystem will output the Malware Distribution graph and distribution information.



Malicious Domain Analysis (3/3)

- 334 malicious domain groups have been generated.
- 17 malicious domain groups were exist in our threat intelligence platform.
- An example of a malicious domain group:



TYPE	ITEM	VIRUSTOTAL
Date	2018_03_29	
Domain	volymum.com	ratio : 4 / 67
	gatyfus.com	ratio : 5 / 67
	gacyzuz.com	ratio : 2 / 67
	youxi.com	ratio : 0 / 64
	gacycaz.com	ratio : 4 / 67
	gadyniw.com	ratio : 5 / 67
	pupydig.com	ratio : 4 / 67
	82.95.66.203	ratio : 0 / 68
	lygysid.com	ratio : 6 / 67
	lygymyn.com	ratio : 5 / 67
Server	217.70.184.38	
	74.206.232.234	
	35.225.160.245	
	50.63.202.71	
	211.151.195.218	
	195.22.4.21	
	104.239.157.210	
	67.55.121.97	
	23.253.126.58	
URL	http://gacyzuz.com/login.php	
	http://youxi.com/mini/mir2/login.php	
	http://gadyniw.com/login.php	
	http://gadyniw.com/tbgZb/YUiQZ/login.php	
	http://agakemegood24.com/login.php	
	http://lyrytyx.com/login.php	
	http://gadyniw.com/YUiQZ/login.php	
	https://203/src/login.php	
	http://gadyciz.com/login.php	
	http://lygymyn.com/login.php	
	http://volymum.com/login.php	
	http://vowykaf.com/login.php