An Investigation into Vulnerability Databases

Bachelor Thesis (final presentation)

31st March 2020

Brian Schweigler

Used Terms

provider

organization and people behind a vulnerability database

vulnerability report

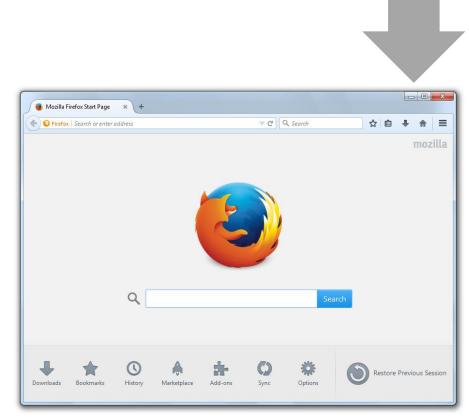
a vulnerability, an exploit, or a security-related document submitted to a provider

severity

potential impact of a vulnerability

libraries with security flaws

Gecko HTML renderer / Australis XUL GUI / ...





		Inbox - Mozilla Thunder	bird			-	a ×	
ew <u>G</u> o <u>M</u> es	age <u>T</u> ools <u>H</u> elp							
👻 🖋 Write	🗬 Chat 🛛 🚨 Address Book 🛛 🤏	Tag 👻 🔍 Quick Filter	Search <ctrl+k></ctrl+k>				٩	
@gm	ail.com 🌪 Quick Filter: 👓 Unr	ead 🚖 Starred 🛔 Contact 🦻 Tags 🖉 Attachment			Filter these messages	<ctrl+shift+k></ctrl+shift+k>	۶	
111)	ኑ \star 🖉 Subject		•• From		Ú 1	Date	_ E	
		Multilizes (Arts 199	 Windows Live 	e Team		12/4/2010 1:02 PM		
1ail	2 1000 (1000 000)	#italakkaa (Barupa) (Witalikaa (Enar))	 Windows Live 	e Team	 12/4/2010 1:02 PM 			
·	☆ • *****		 Xbox 	 Xbox 		 12/9/2010 5:50 PM 		
		ennelle i Rekonsti yapose i Anne saarii i Annee i Rekonsti PARI	 Xbox 		 12/10/2010 7:18 PM 12/17/2010 4:48 PM 			
		Hilli yanta i afkan yan iling ya anta i Windon i Pinan il	 Xbox 					
		HARLINGS FOR FROM FILMER	MICROSOFT *XBOX LIVE Xbox		 12/19/2010 10:13 PM 12/23/2010 3:48 PM 			
			Xbox LIVE		 12/25/2010 11:23 AM 			
	☆ · ··································	a - Hengan - Hengan Photosof	Xbox		•	12/30/2010 1:30 PM		
:		Thunderbird	 New features More tips 	SVisit our Blog	Contribute			
					Q oct hop			
	🛖 Add	Add-on of the Week: Dropbox for FileLink			Need Support?			
	Add Dropbox	Add Dropbox support to Thunderbird's Filelink feature. Thunderbird's Filelink feature makes it quick and easy to send large attachments by uploading those attachments to various storage services and		Over 75% of Thunderbird support questions are answered on the Knowledge Base.				
				If you can't find an answer, ask your question at Get Satisfaction.		on.		
		g a link to the file into the body of your email.	Learn More »					
	Get Dropfox	for FileLink »						
nderbird is f	ree and open source software from t	he non-profit Mozilla Foundation.				Know your r	rights >	
					1	Unread: 111	Tatal 11	



libraries with security flaws

mpg123 / ffmpeg / ...

WINAMP	WINAMP PLAYLIST		🗃 Windows Media Player
* * : : : : : : : : : : : : : : : : : :	1. Depeche Mode - Never Let Me Down Again	4:47	File View Play Favorites Go Help
128 kbps 44 kHz mono share	2. Depeche Mode - The Things You Said 3. Depeche Mode - Strangelove	4:02 4:54	🖛 🔿 🦓 Radio 🏚 Music 📸 Media Guide
	4. Depeche Mode - Sacred	4:48	
	5. Depeche Mode - Little 15	4:18	
K 🗅 II 🗖 🕅 📥 FSHUFFLE 🕰 🏈	6. Depeche Mode - Behind The Wheel	5:17	
	7. Depeche Mode - I Want You Now	3:38	
WINAMP EQUALIZER	8. Depeche Mode - To Have And To Hold	2:56	
FON FAUTO	9. Depeche Mode - Nothing	4:17	Windows
	10. Depeche Mode – Pimpf 11. Depeche Mode – Agent Orange	5:25 5:04	windows
	12. Depeche Mode - Never Let Me Down Again .		Media [™]
		×	
	ADD REM SEL MISC 0:00/54:22+	LIST	
PREAMP 60 170 310 600 IK 3K 6K 12K 14K 16K	K►11¥X▲ 01:00		<u>.</u>



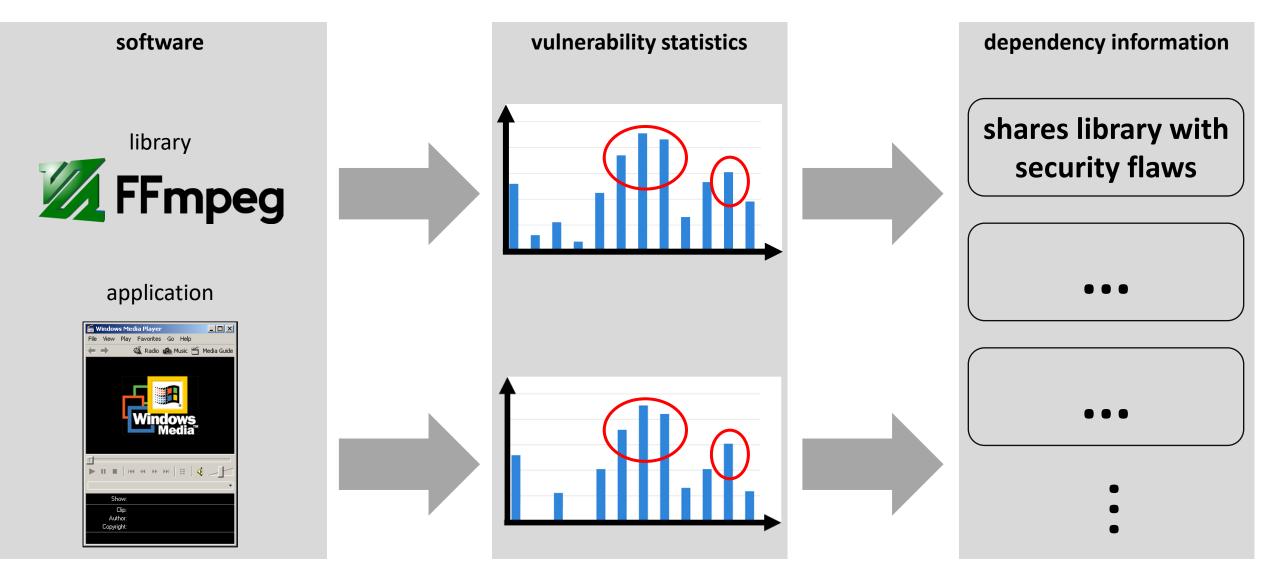


Show: Clip: Author: Copyright:



... but how can we leverage vulnerability databases?

Our Idea



What Do We Need to Know?

RQ1

What are the **affiliations** between the different vulnerability database providers, and **what data** do they collect?

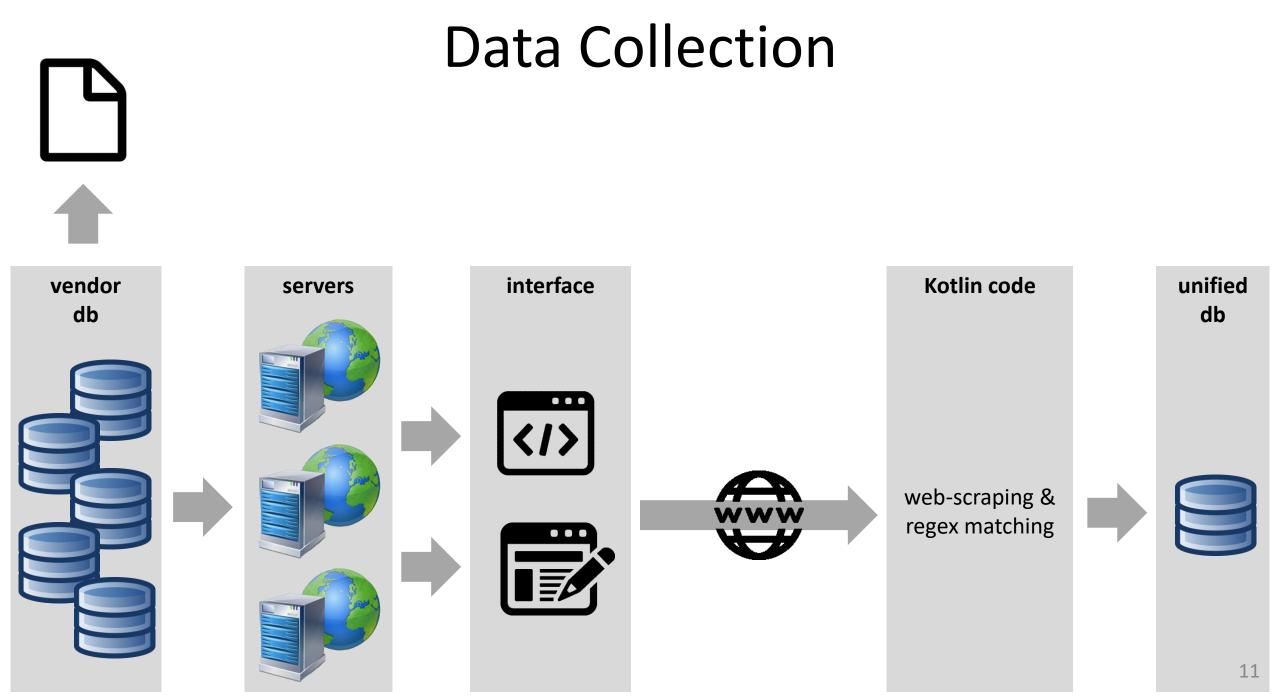
First, we need data!

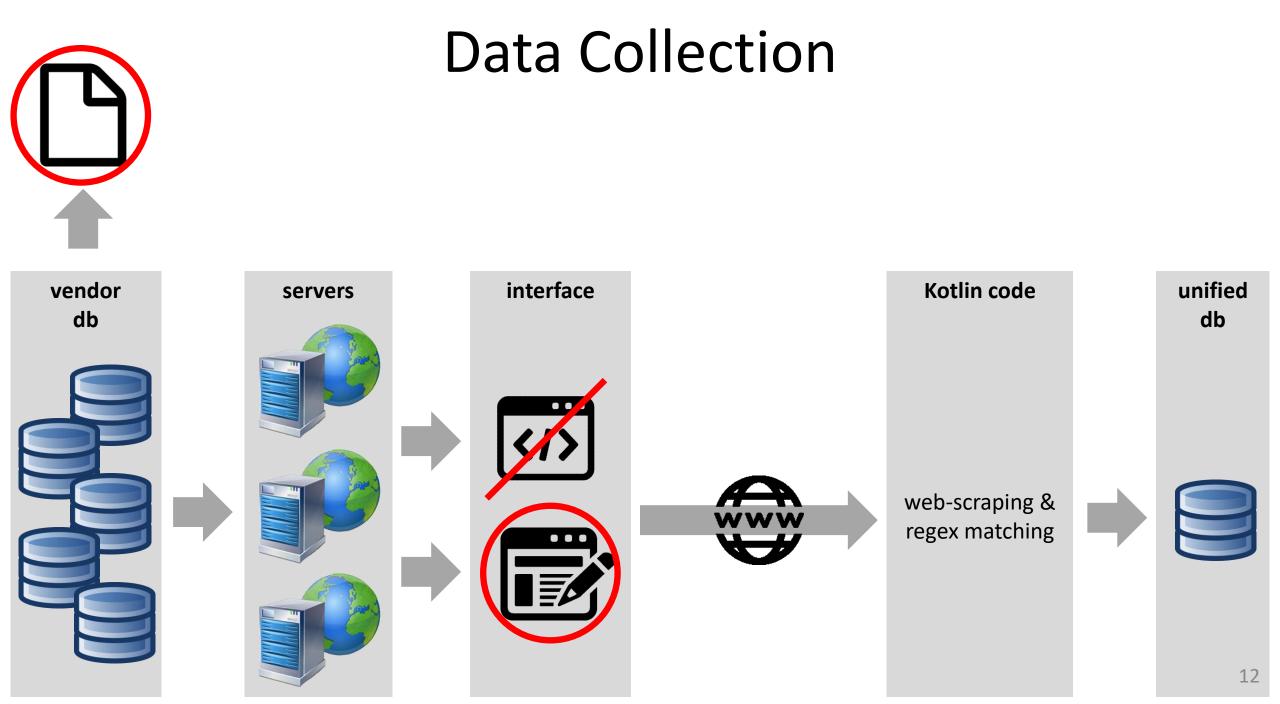
First, we need data!

LOTS of data.

Evaluated Providers

Provider	Free	Founded in	Owner	Source	Remarks
CVE	yes	1999	Mitre	open	simple, unbiased overview
Exploit-DB	yes	2004	Offensive Security	open	exploit and app download
NVD	yes	2000	NIST	closed	lists affected software
RAPID7	no	2000	RAPID7	closed	evaluates package use
Snyk	yes	2006	Snyk Ltd.	closed	evaluates package use





Data Processing

Python scripts applied to vulnerability descriptions for ...

tokenizing strings

counting word frequencies in descriptions

grouping by dates

removing stop-words

plotting (140+)



Exploit-DB requires a valid HTTP header for requests User-Agent: <product> / <product-version>

Exploit-DB requires regular IP address changes

character set encoding issues
(who needs special characters?!)

Our Dataset

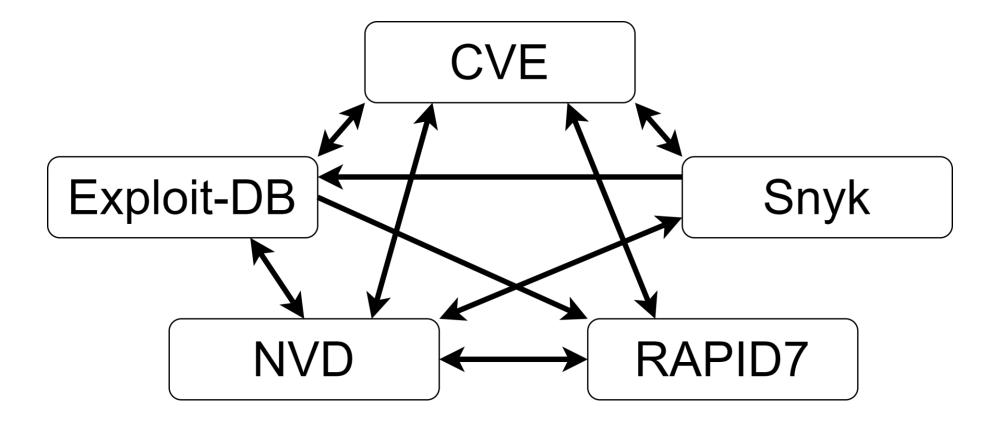
Provider	First Report	Cut-off date	# Entries
CVE	1999	12.12.2019	156,828
NVD	1999	03.12.2019	133,477
Exploit-DB	1988	01.11.2019	44,539
RAPID7	2004	18.12.2019	30,849
Snyk	2005	17.11.2019	4,605

What Do We Need to Know?

RQ1

What are the **affiliations** between the different vulnerability database providers, and **what data** do they collect?

Vulnerability Provider Affiliations



Supported Feature Sets



What Do We Need to Know?

RQ1

What are the **affiliations** between the different vulnerability database providers, and **what data** do they collect?

RQ2

Are the vulnerability scoring systems used consistently?

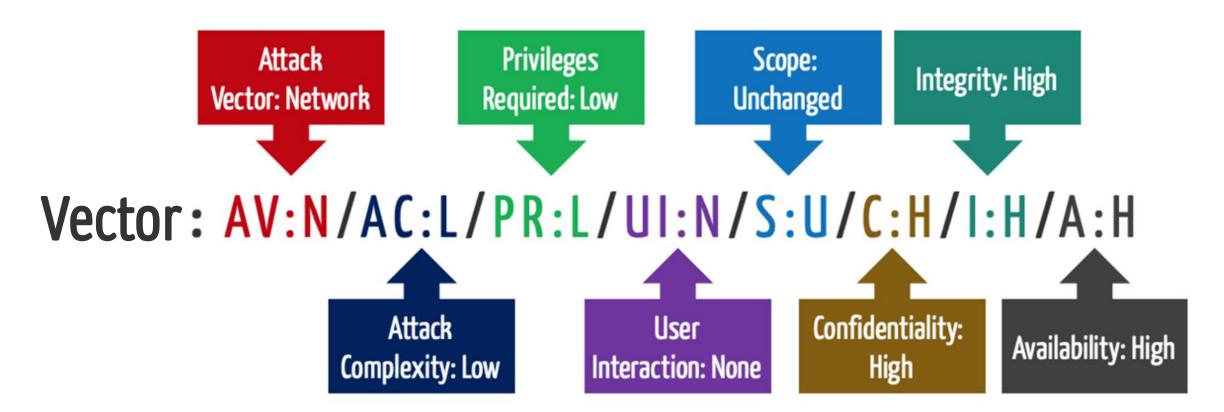
Scoring

"The Common Vulnerability Scoring Standard (CVSS) provides a way to capture principal characteristics of a vulnerability and produce a numerical score [1-10] reflecting its severity."

- FIRST (Forum of Incident Response and Security Teams)

CVSS Details

multiple versions are in use (CVSS V2, CVSS V3, CVSS V3.1)



Scoring

Provider	CVSS V2	CVSS V3	V2 Average	V3 Average
CVE	×	×	n/a	n/a
NVD			6.2	7.4
Exploit-DB			n/a	n/a
RAPID7		×	6.3	n/a
Snyk			n/a	6.6

What Do We Need to Know?

RQ1

What are the **affiliations** between the different vulnerability database providers, and **what data** do they collect?

RQ2

Are the vulnerability scoring systems used consistently?

RQ3

Can we see trends based on the collected data?

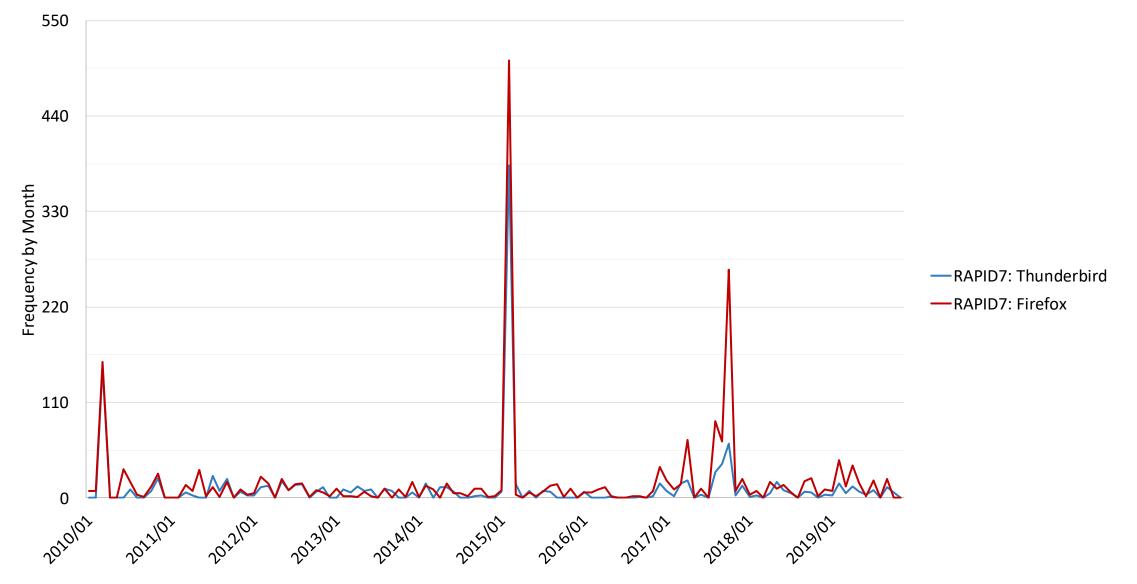
Determination of Affected Software

200 most frequent non-stop words found in the descriptions: (filtered by software names)

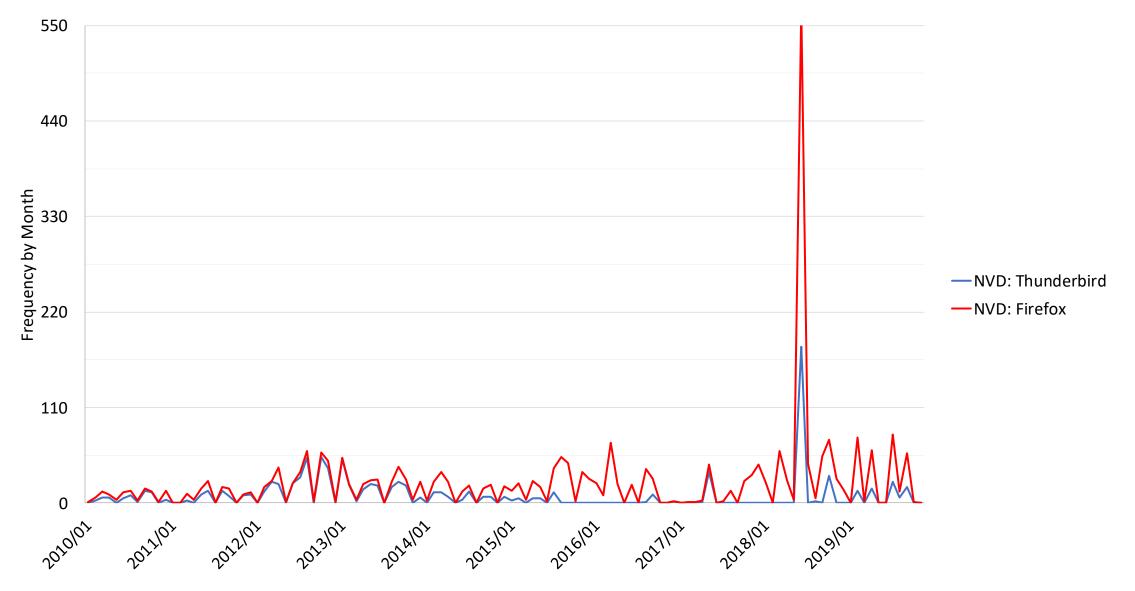
Acrobat, Android, Apache, Apple, Chrome, Chromium*, FFmpeg*, Flash, Firefox, Java, Linux, Thunderbird, Windows, Wordpress

... and then we created some plots!

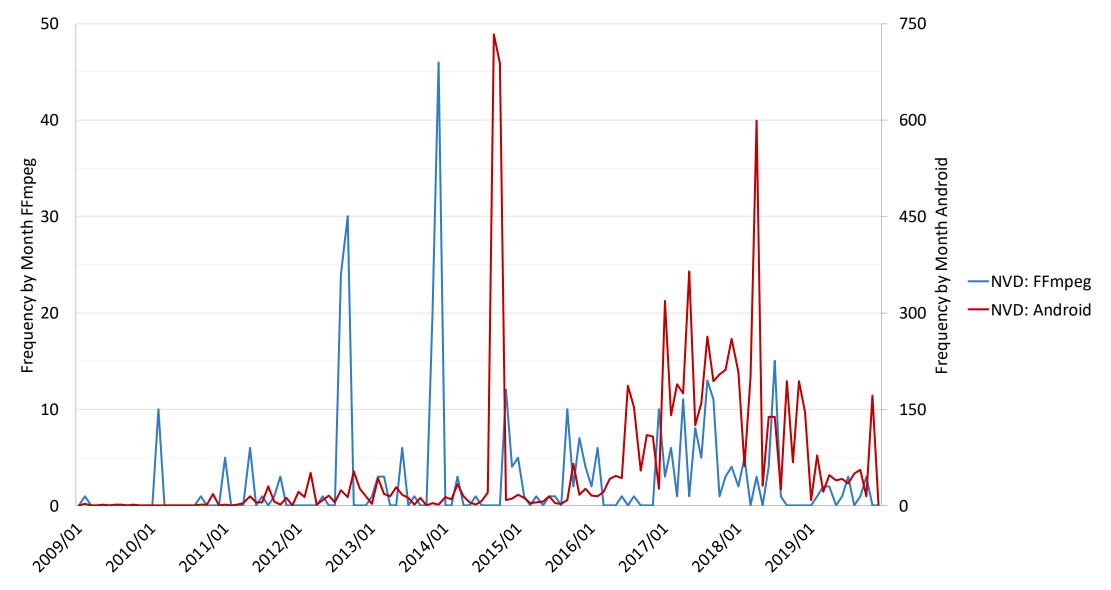
Trends - Shared Code (Thunderbird / Firefox)



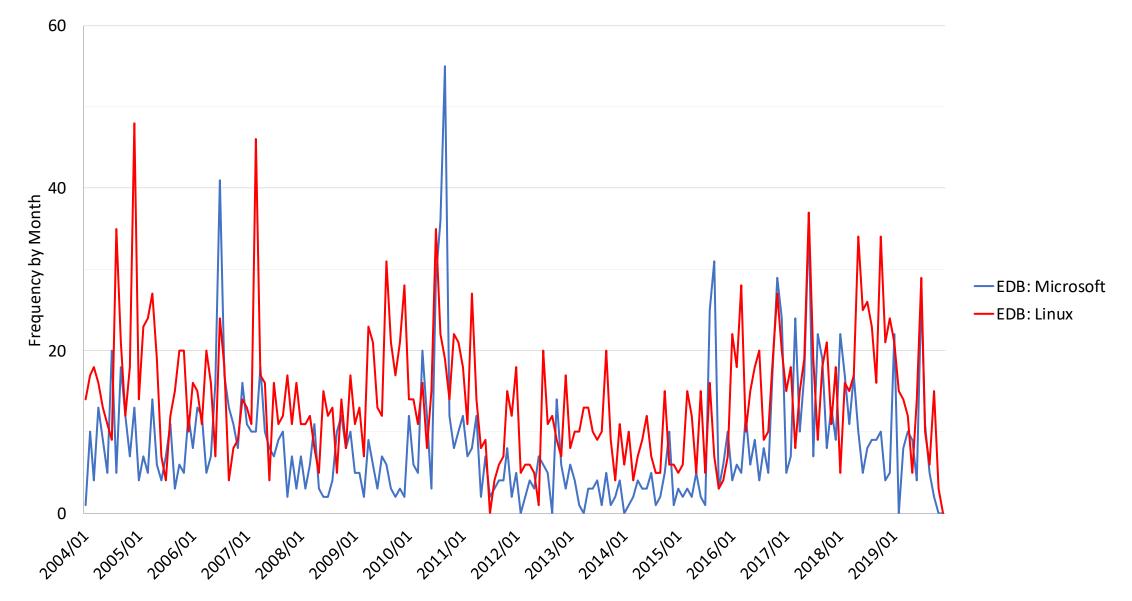
Trends - Shared Code (Thunderbird / Firefox)



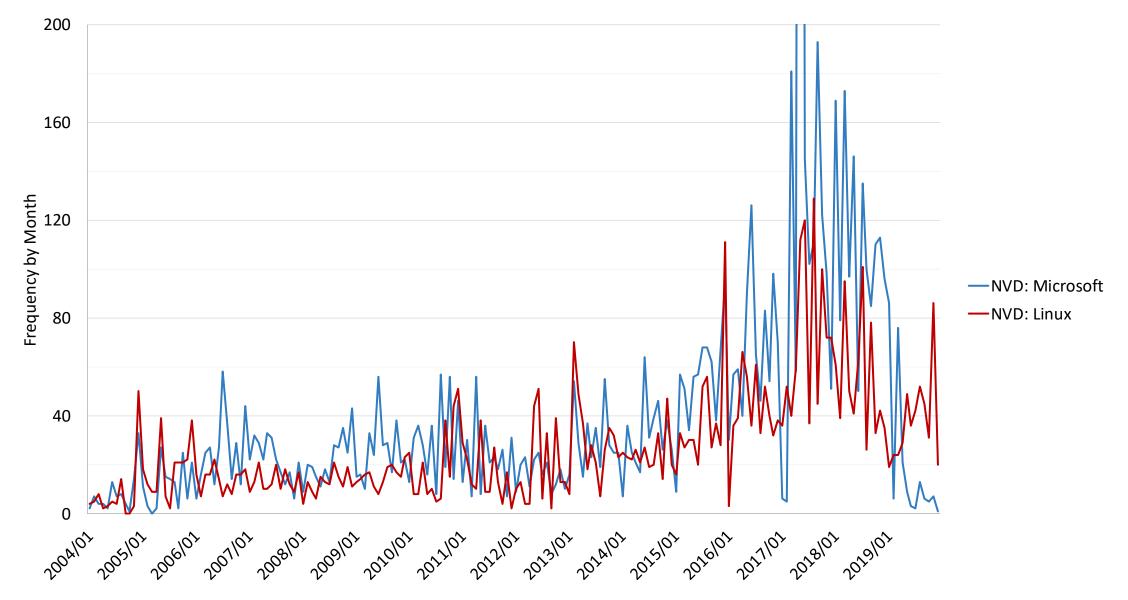
Trends - Shared Code (FFmpeg / Android)



Trends - Related Software (Microsoft / Linux)



Trends - Related Software (Microsoft / Linux)

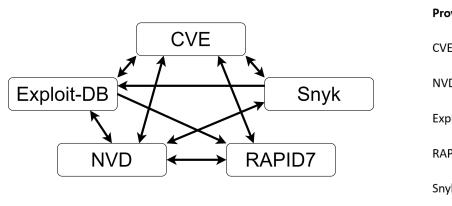


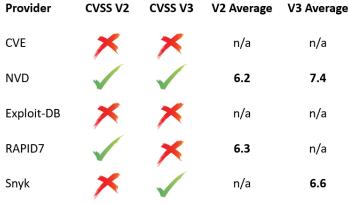
Future Work

machine learning to find corresponding patterns

improved NLP on descriptions

Summary





RQ1: Affiliations & Data RQ2: Scoring

RQ3: Trends