ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS

Northeastern University

A Broad View of the Ecosystem of Socially Engineered Exploit Documents

Stevens Le Blond, Cédric Gilbert, Utkarsh Upadhyay,
Manuel Gomez Rodriguez and **David Choffnes**

Challenges with measuring targeted attacks

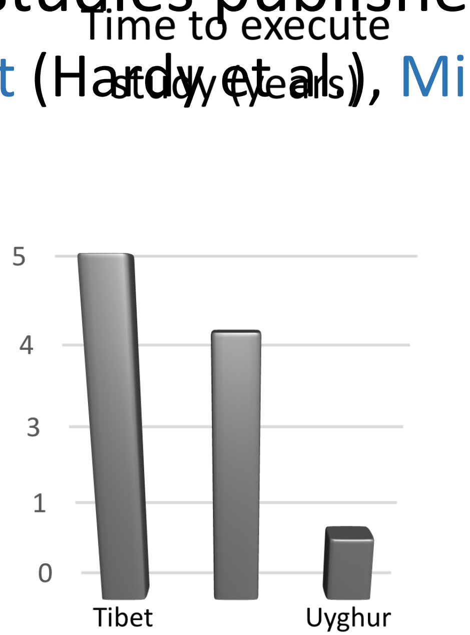
- Low-volume, socially engineered messages that convince specific victims to install malware

Challenges with measuring targeted attacks

- Low-volume, socially engineered messages that convince specific victims to install malware
- Three studies published at Usenix Security'14
  - Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)

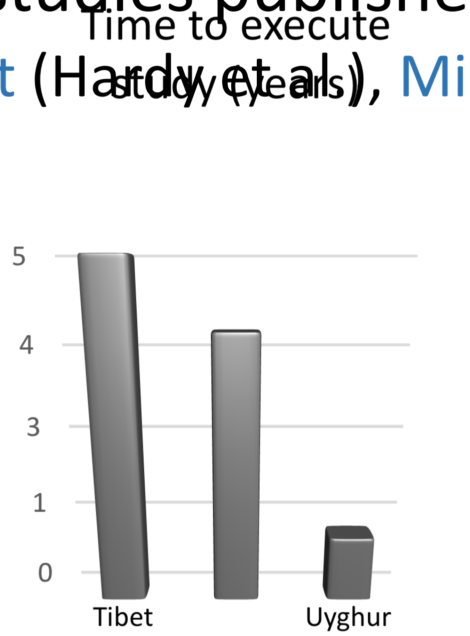
Challenges with measuring targeted attacks

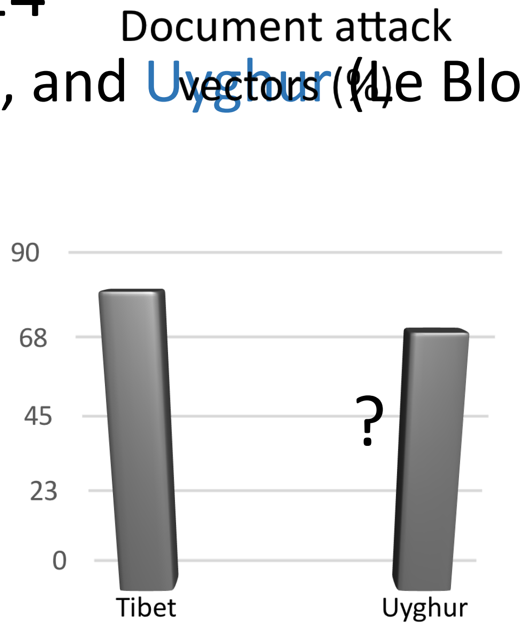
- Low-volume, socially engineered messages that convince specific victims to install malware
- Three studies published at Usenix Security’14
  - Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)



Challenges with measuring targeted attacks

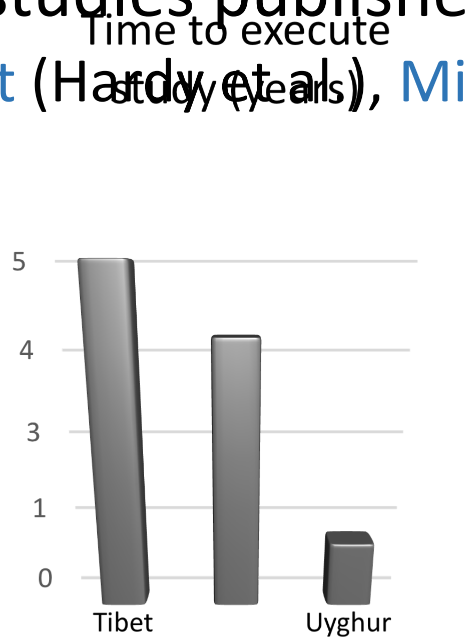
- Low-volume, socially engineered messages that convince specific victims to install malware
- Three studies published at Usenix Security'14
  - Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)

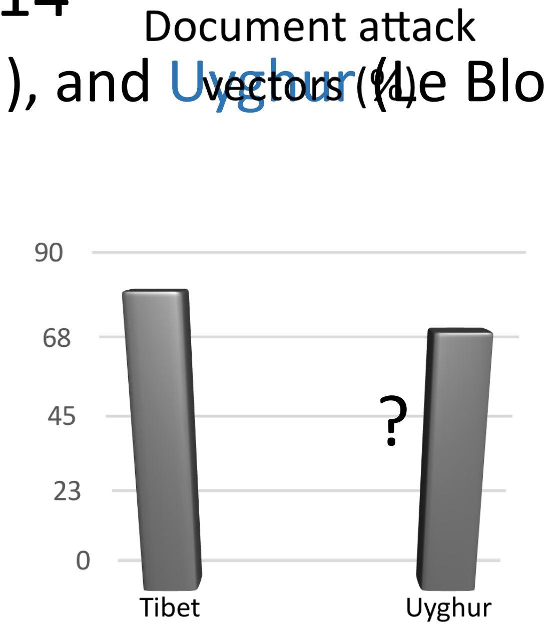




Challenges with measuring targeted attacks

- Low-volume, socially engineered messages that convince specific victims to install malware
- Three studies published at Usenix Security’14
  - Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)

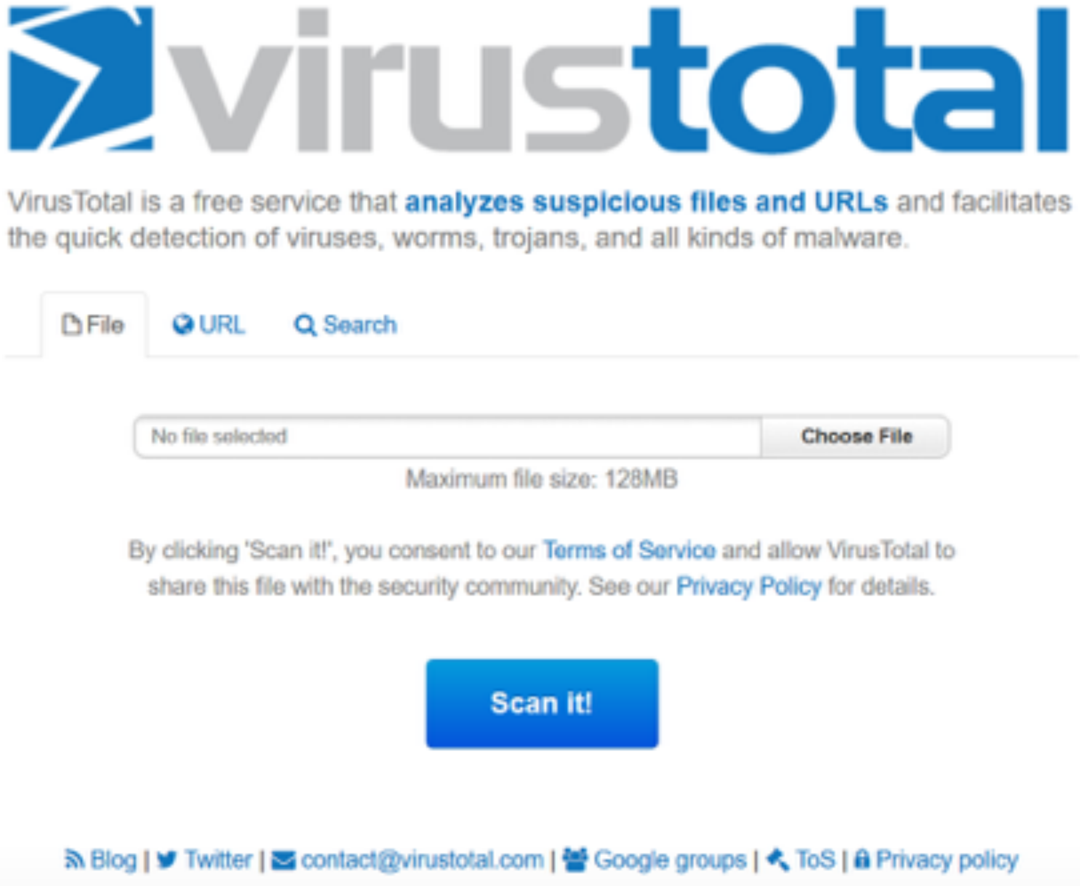




Measuring targeted attacks is a long and difficult process

Can Anti-Virus Aggregators (VirusTotal) help?

Can Anti-Virus Aggregators (VirusTotal) help?



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

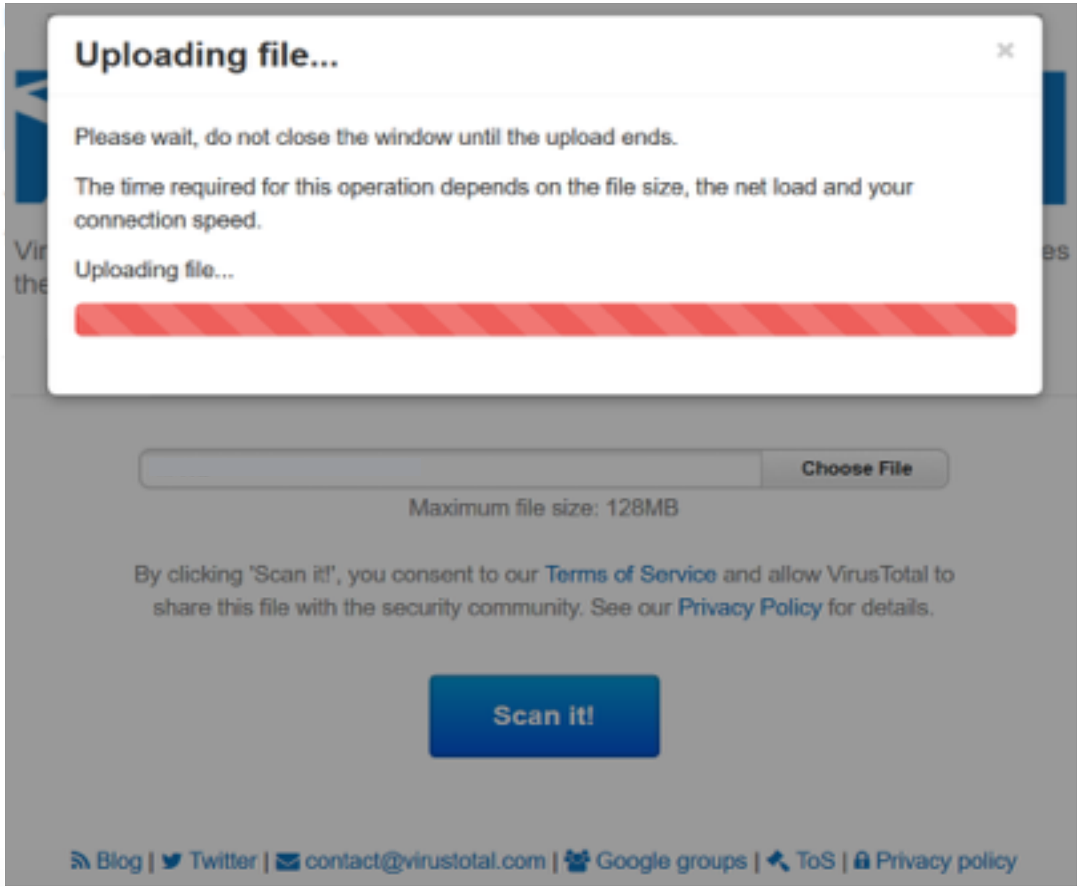
No file selected | Choose File

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Can Anti-Virus Aggregators (VirusTotal) help?



Uploading file...

Please wait, do not close the window until the upload ends.

The time required for this operation depends on the file size, the net load and your connection speed.

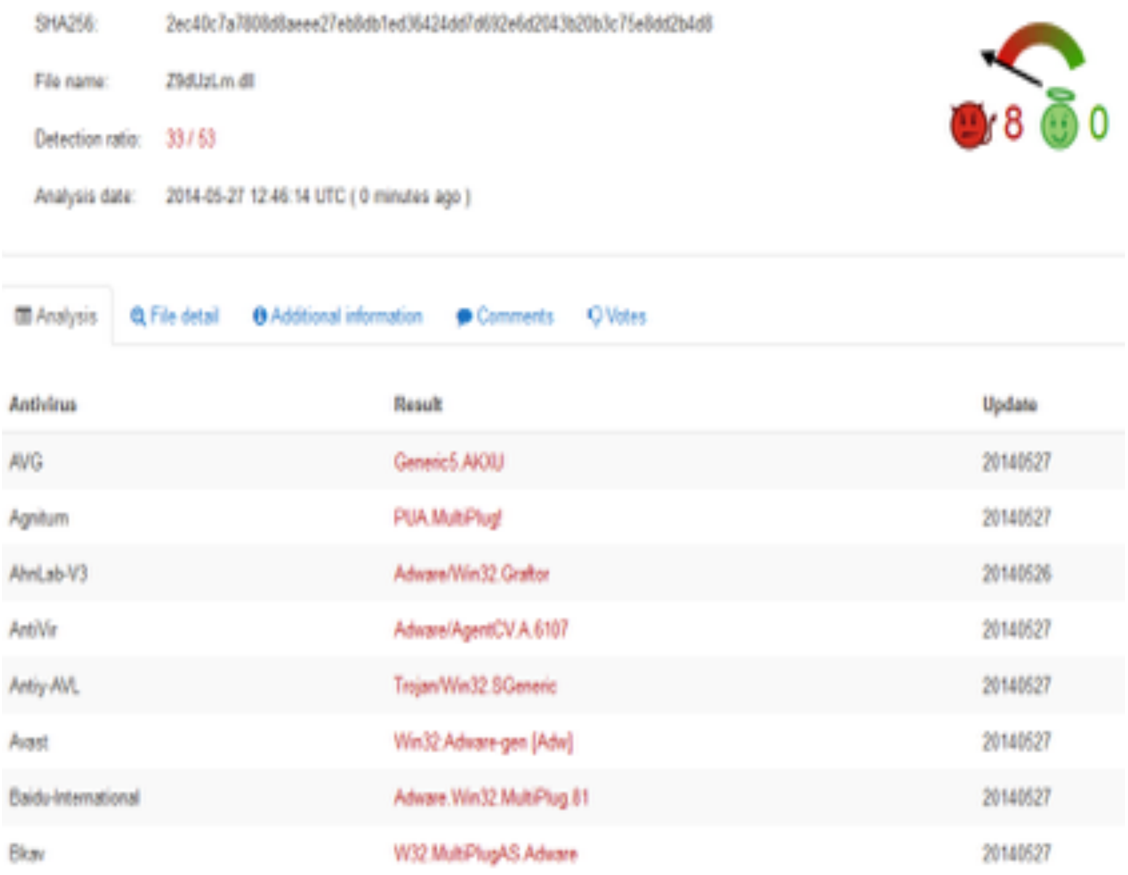
Uploading file...

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Can Anti-Virus Aggregators (VirusTotal) help?



SHA256: 2ec40c7a7808d8aeee27eb8db1ed36424dd7d692e6d2043b20b3c75e8dd2b4d8

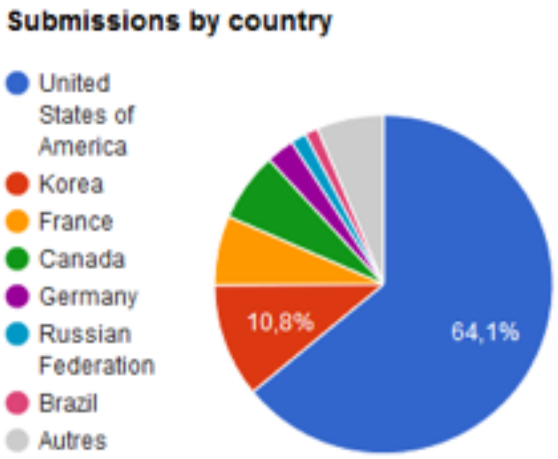
File name: Z9dUzLm.dll

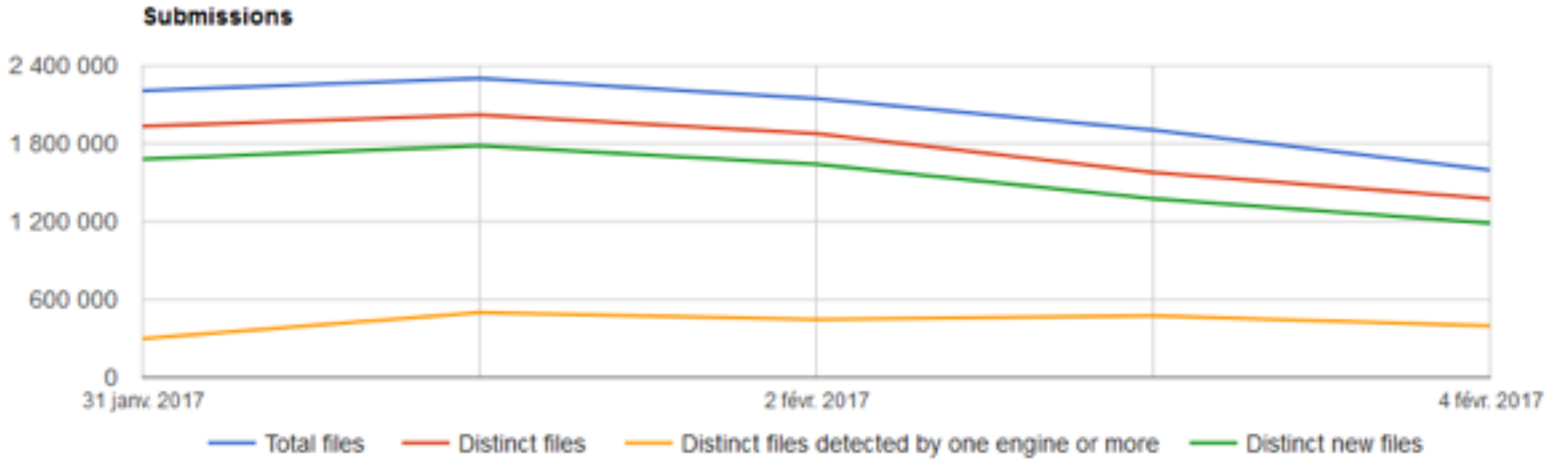
Detection ratio: 33 / 53

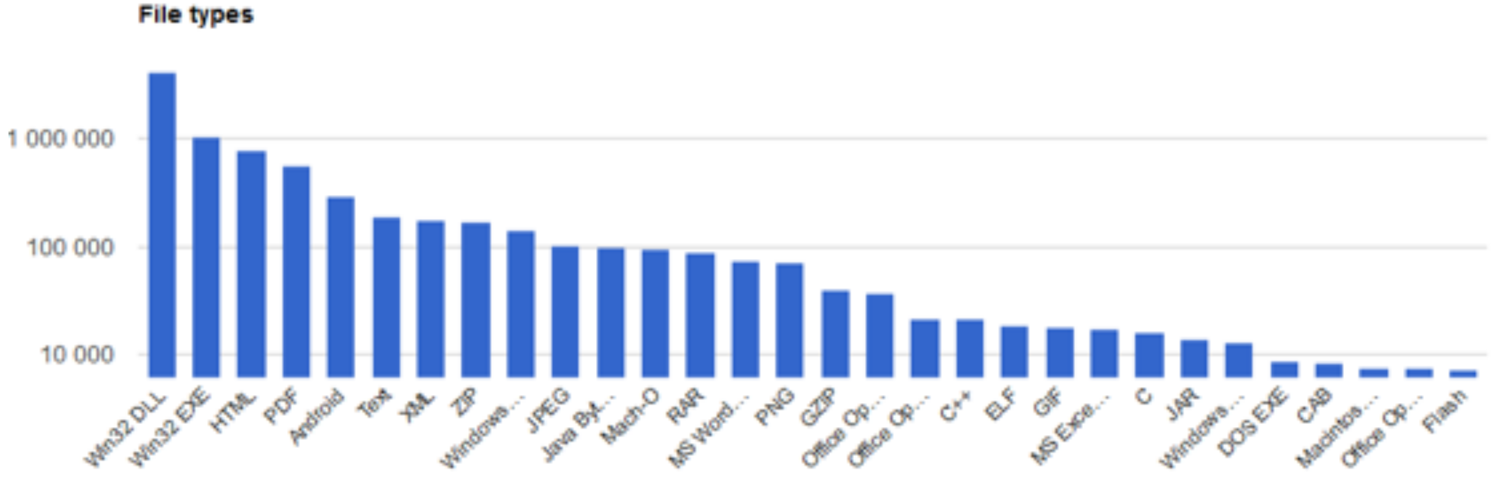
Analysis date: 2014-05-27 12:46:14 UTC (0 minutes ago)

Antivirus	Result	Update
AVG	Generic5.AKXU	20140527
Agnitum	PUA.MultiPlug!	20140527
AhnLab-V3	Adware/Win32.Graftor	20140526
AntiVir	Adware/AgentCV.A.6107	20140527
Antiy-AVL	Trojan/Win32.SGeneric	20140527
Avast	Win32:Adware-gen [Adw]	20140527
Baidu-International	Adware.Win32.MultiPlug.81	20140527
Bkav	W32.MultiPlugAS.Adware	20140527

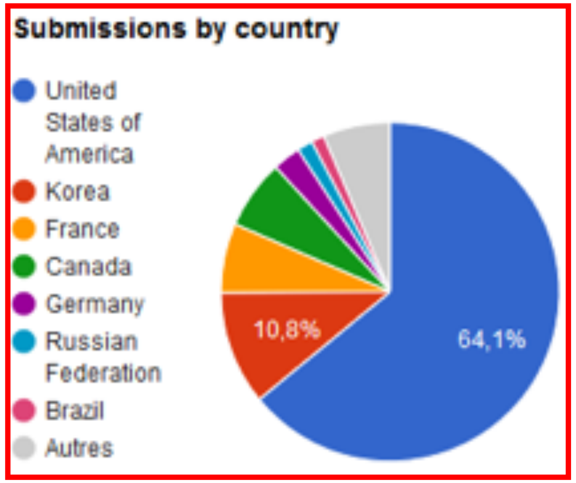
VirusTotal Statistics (one week)



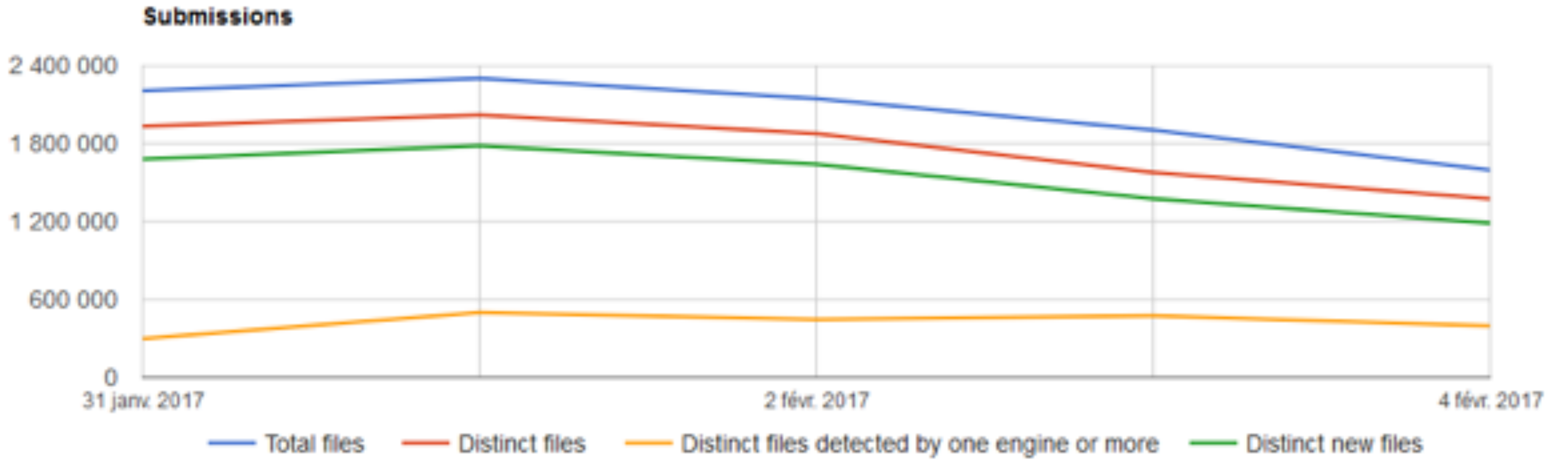




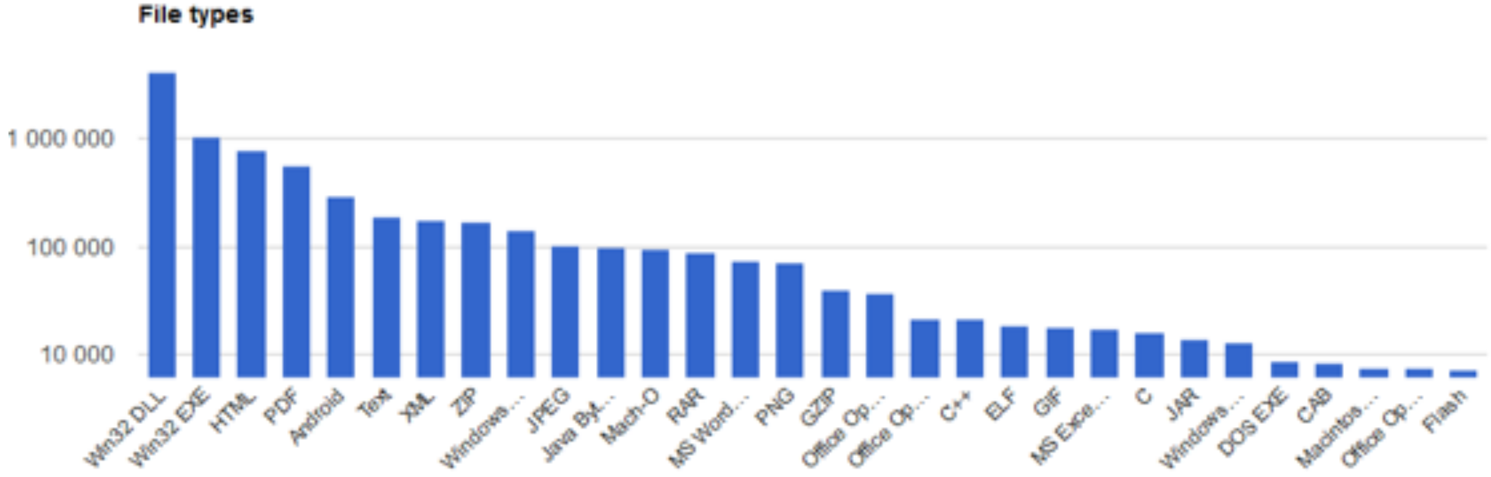
VirusTotal Statistics (one week)



Submissions by country

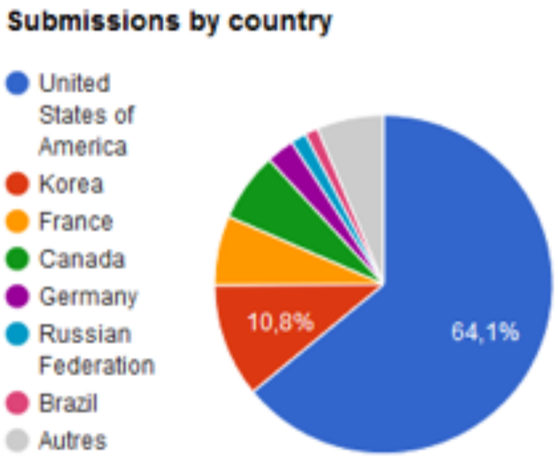


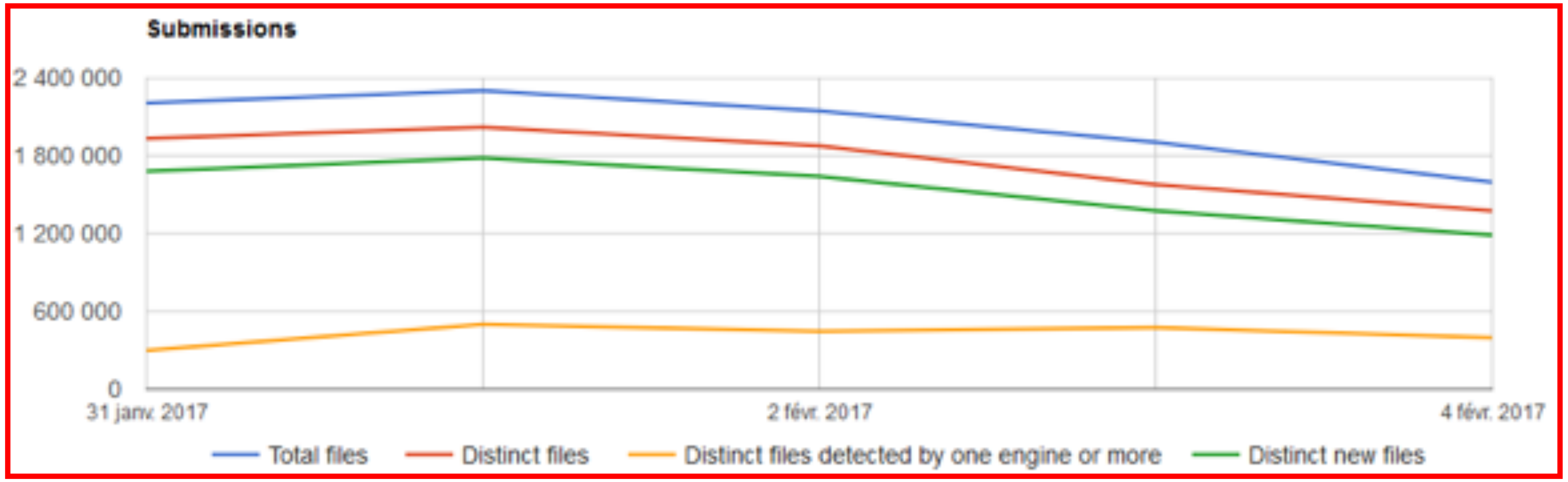
Submissions

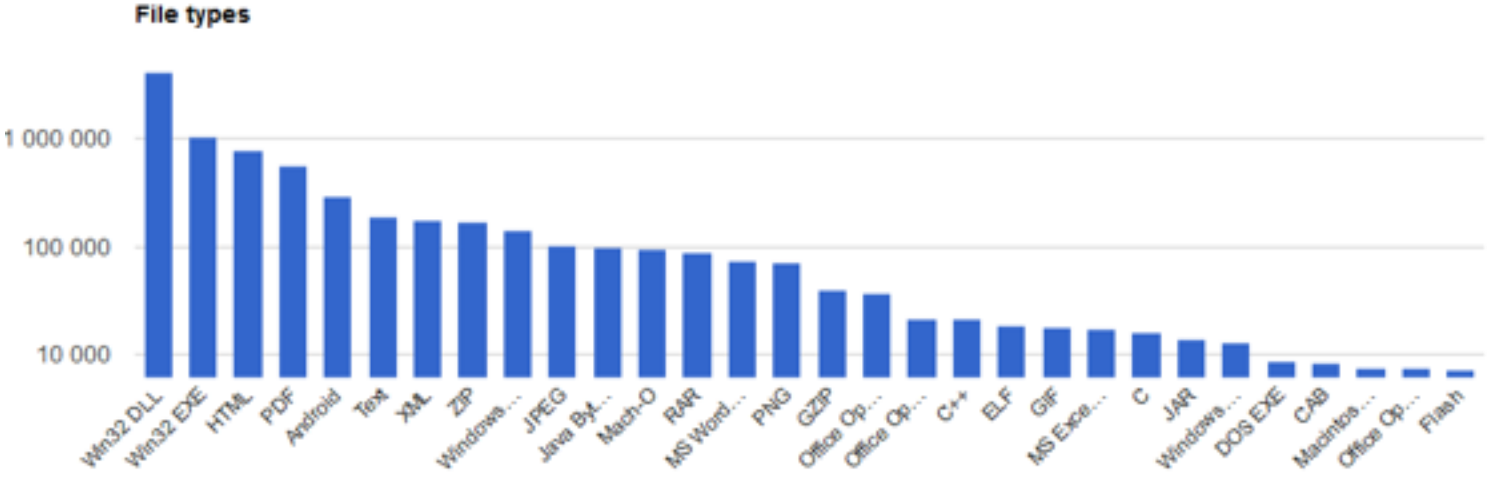


File types

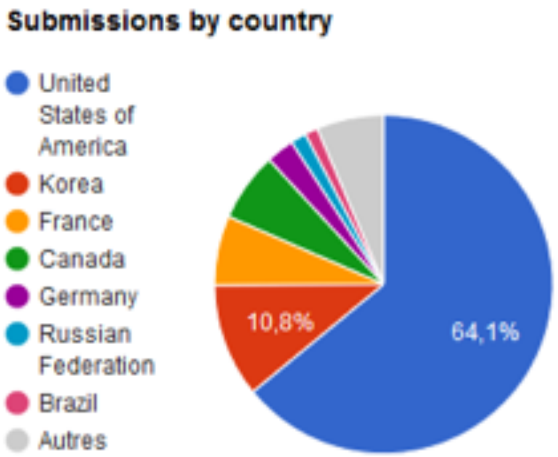
VirusTotal Statistics (one week)

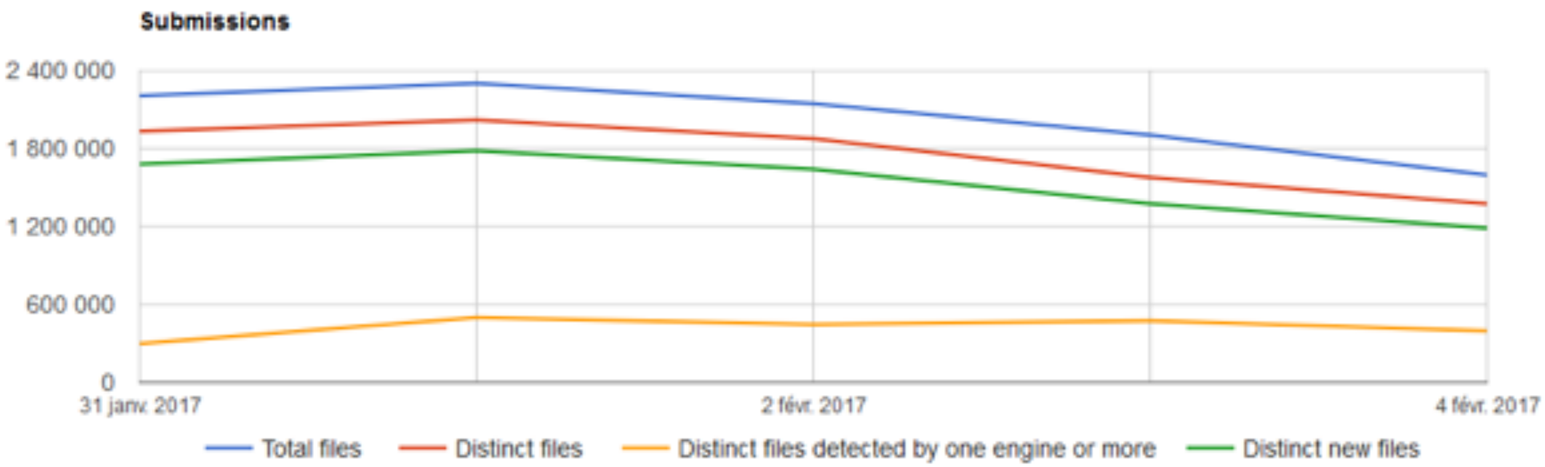


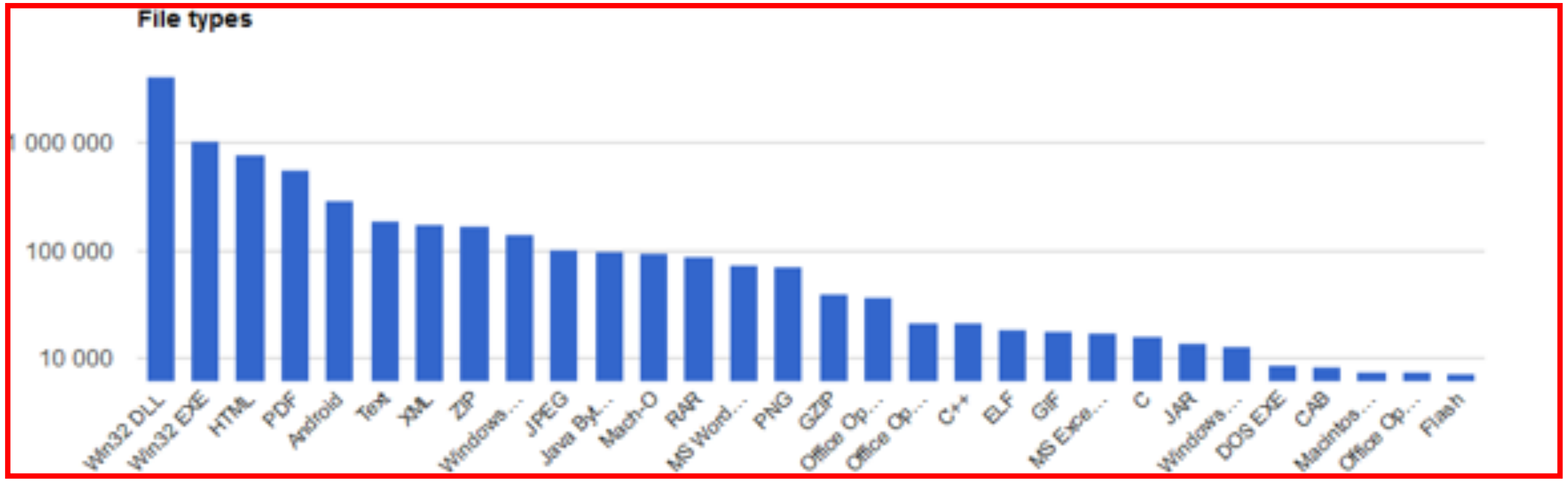




VirusTotal Statistics (one week)

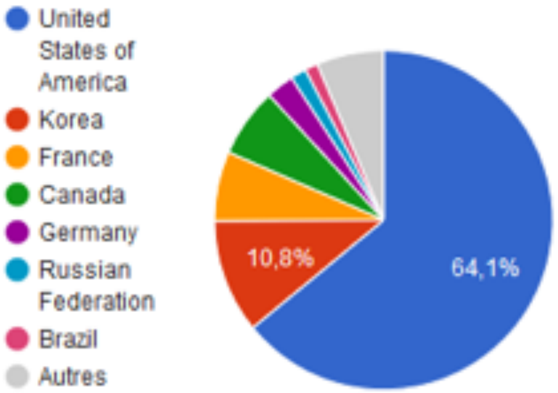

Submissions by country


Submissions

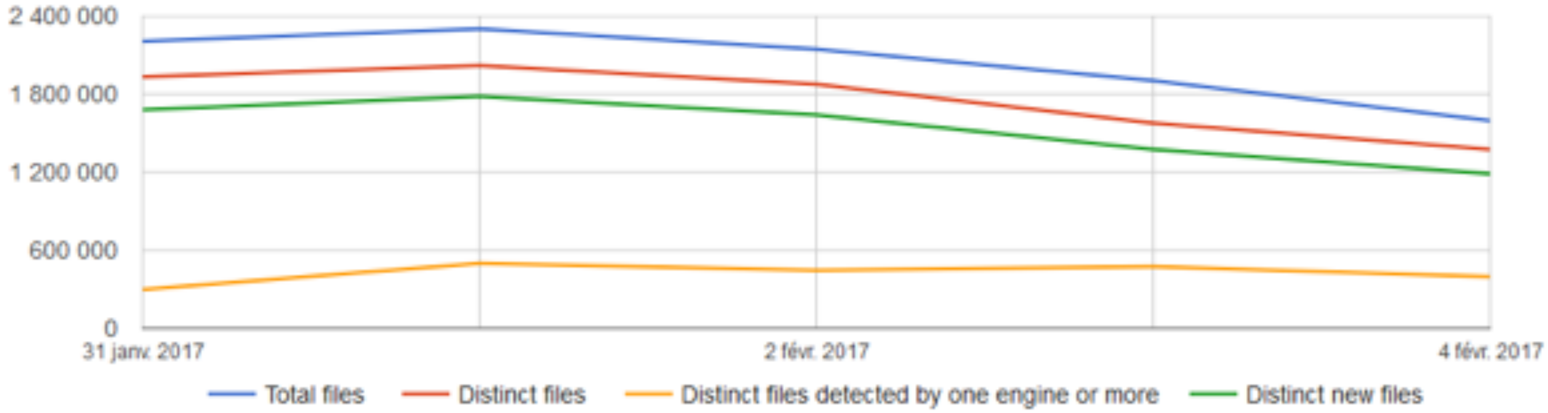

File types

VirusTotal Statistics (one week)

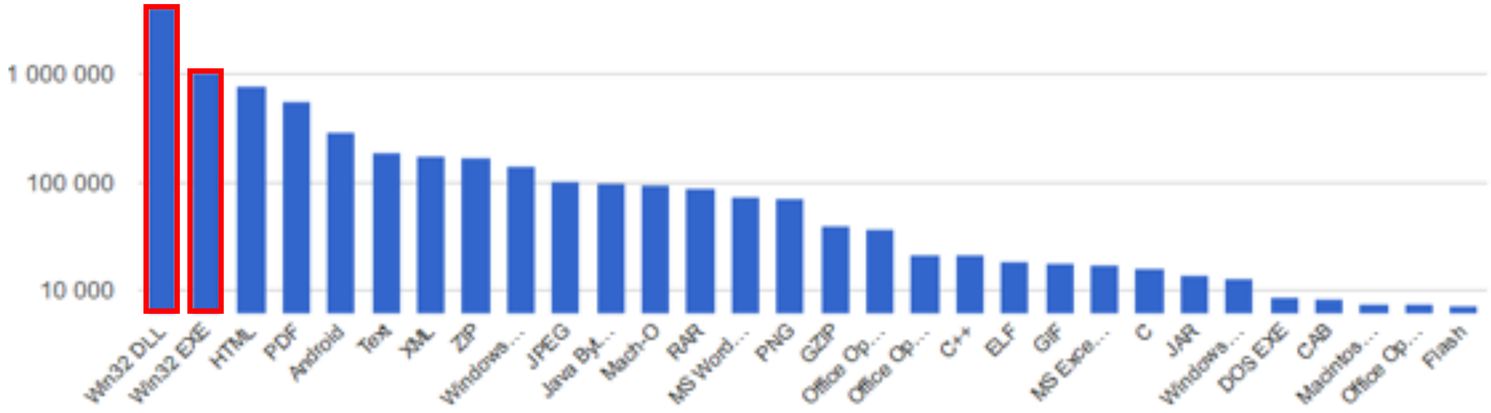
Submissions by country



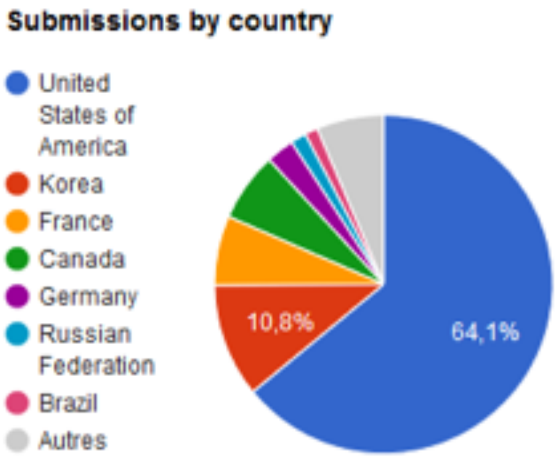
Submissions



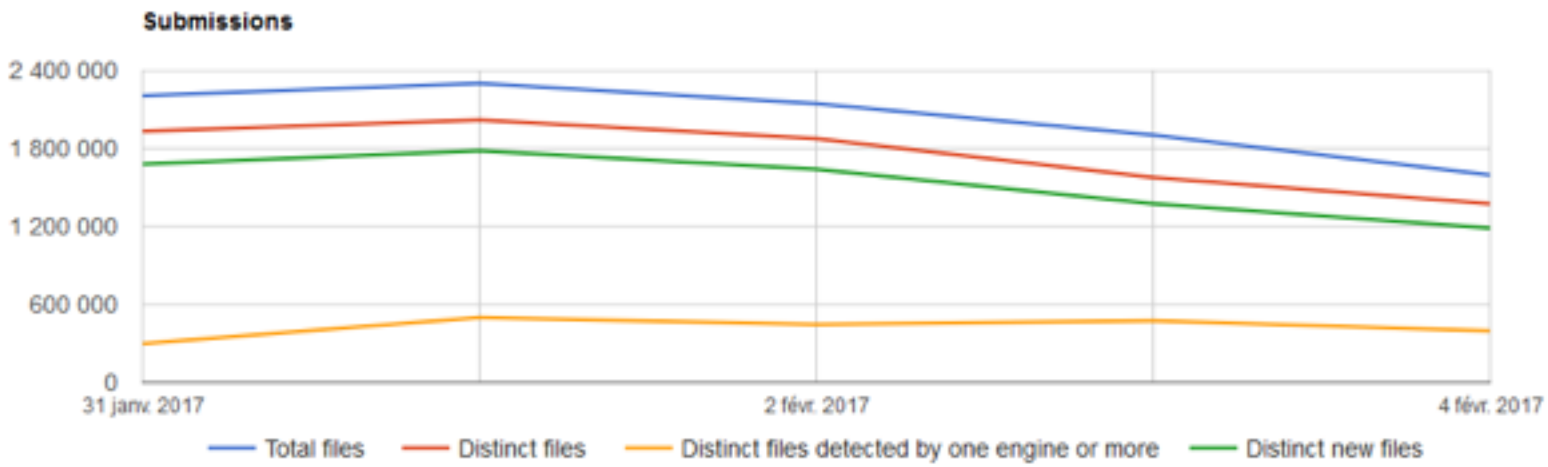
File types



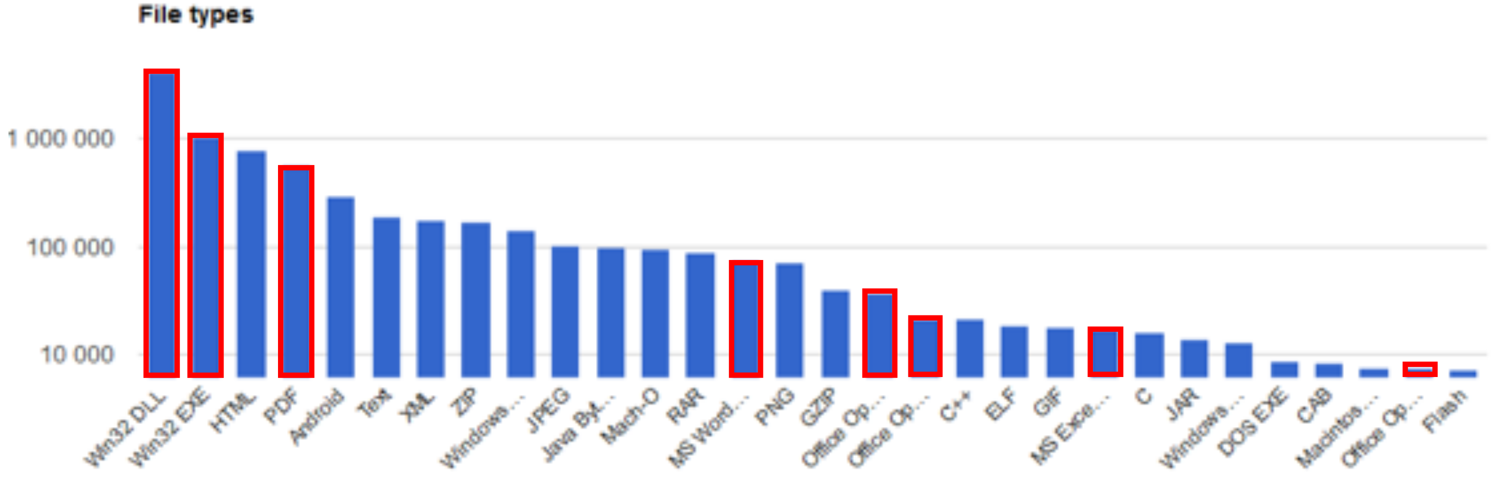
VirusTotal Statistics (one week)



Submissions by country



Submissions



File types

VirusTotal as a vantage point to measure targeted attacks

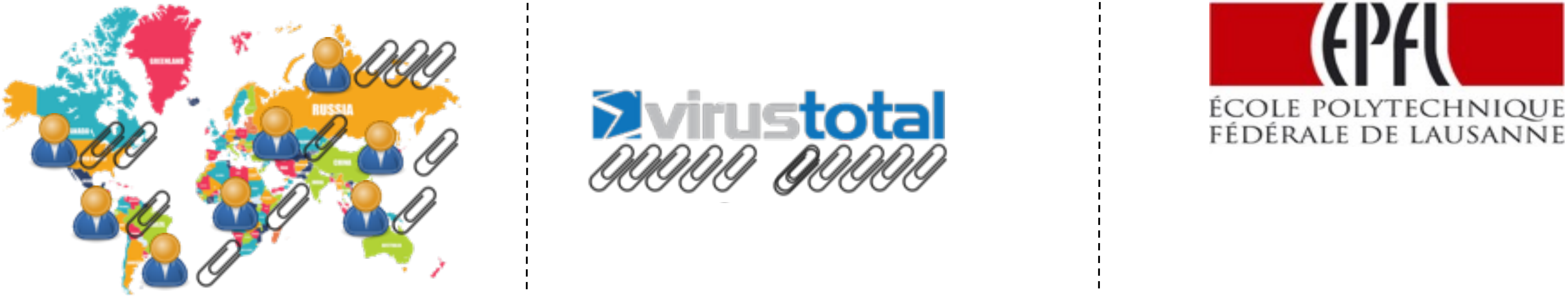
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

VirusTotal as a vantage point to measure targeted attacks

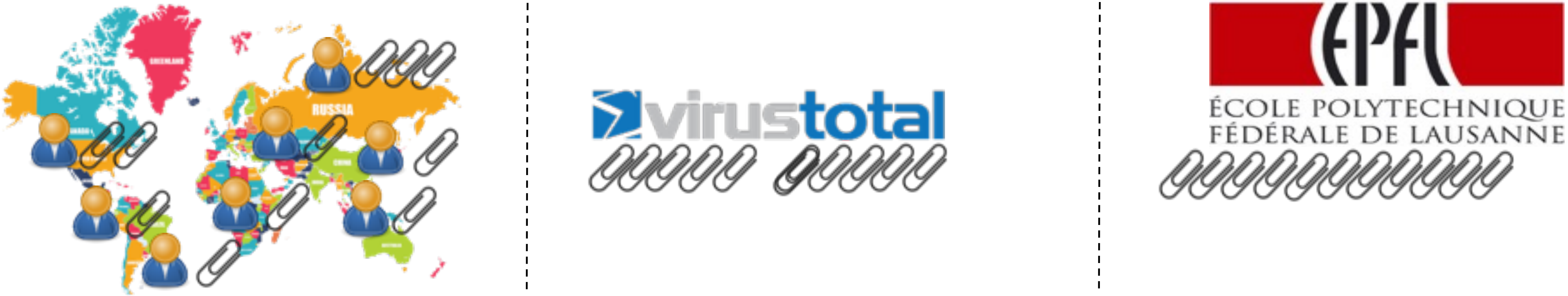
virustotal

EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

VirusTotal as a vantage point to measure targeted attacks



VirusTotal as a vantage point to measure targeted attacks



Research questions

- Do targeted groups upload exploit documents to VirusTotal?
- Can we scale our analysis to hundreds of thousands of samples?
- How do attacks faced by different groups compare with each other?
- Is VirusTotal used by other actors such as attackers and researchers?

Outline

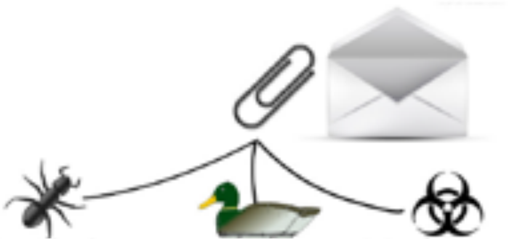
1) Methodology

2) Analysis of exploit documents

3) Future work

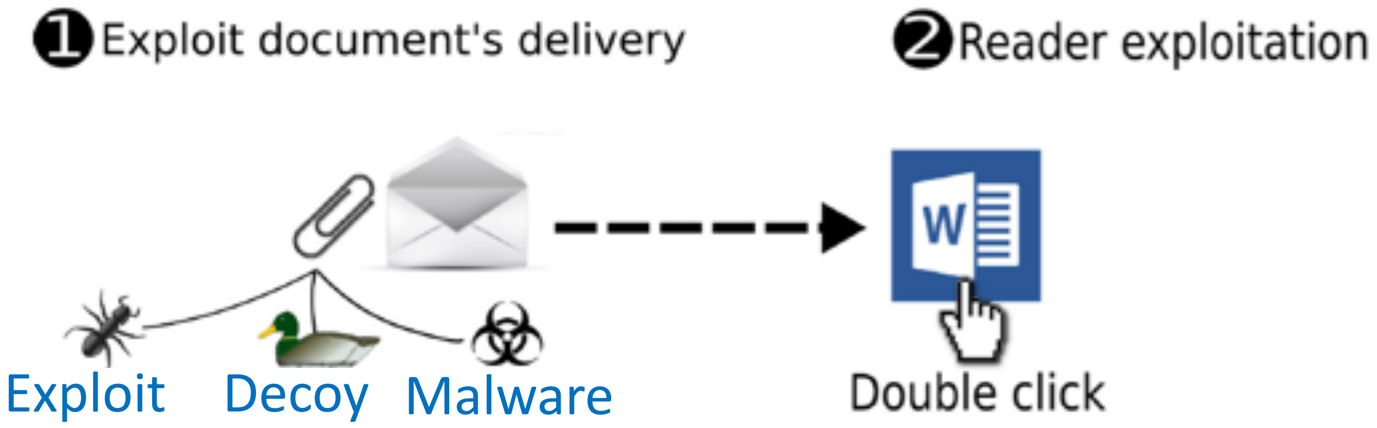
Exploit document infection process

❶ Exploit document's delivery

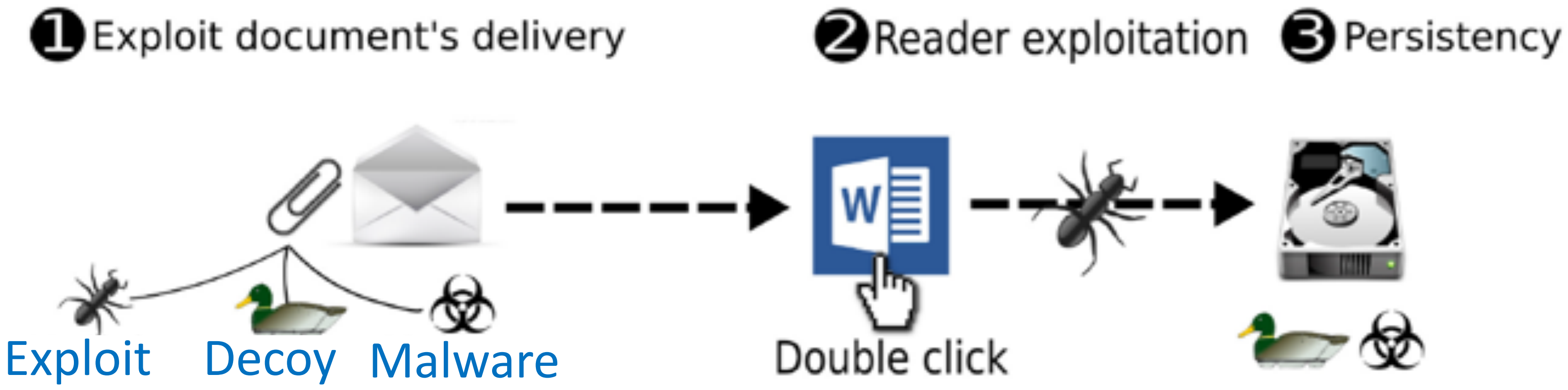


Exploit Decoy Malware

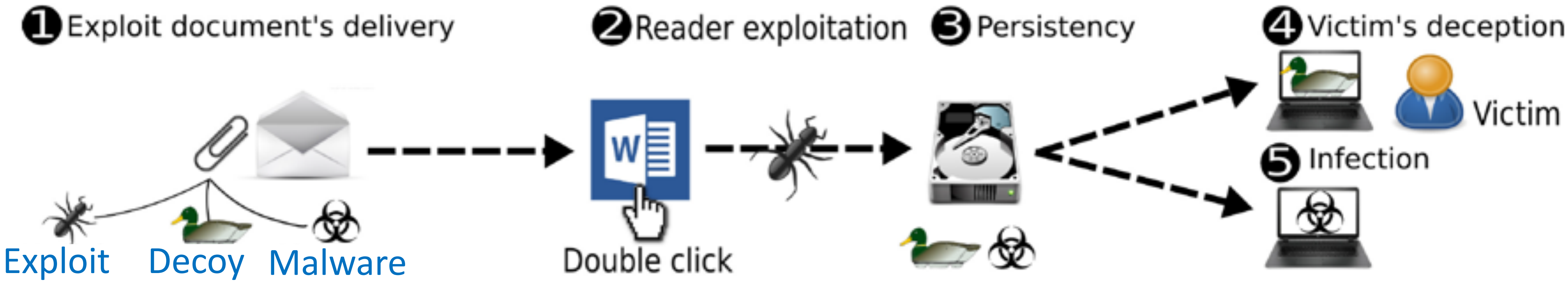
Exploit document infection process



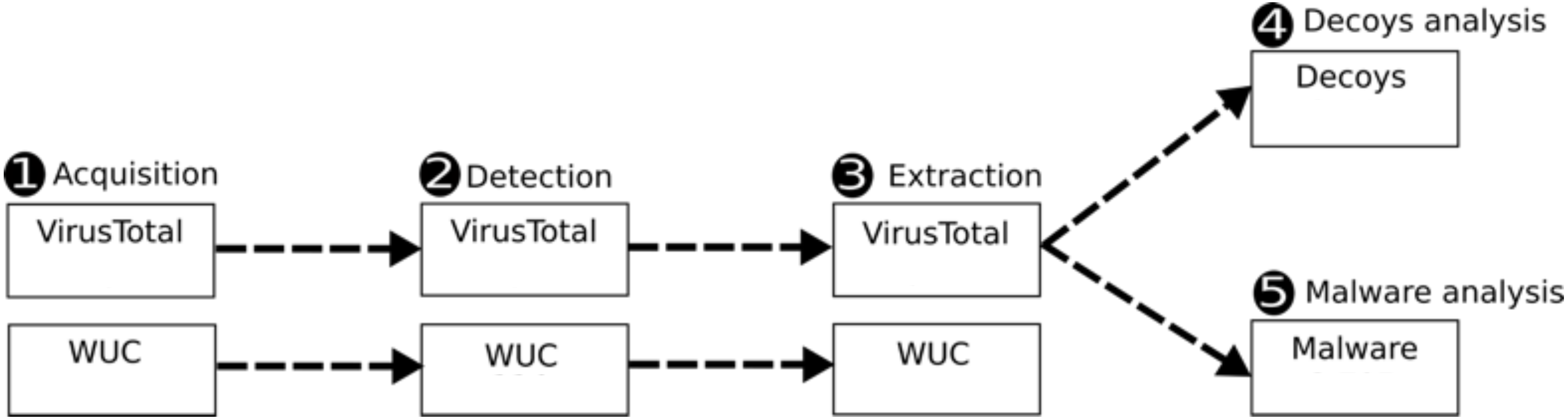
Exploit document infection process



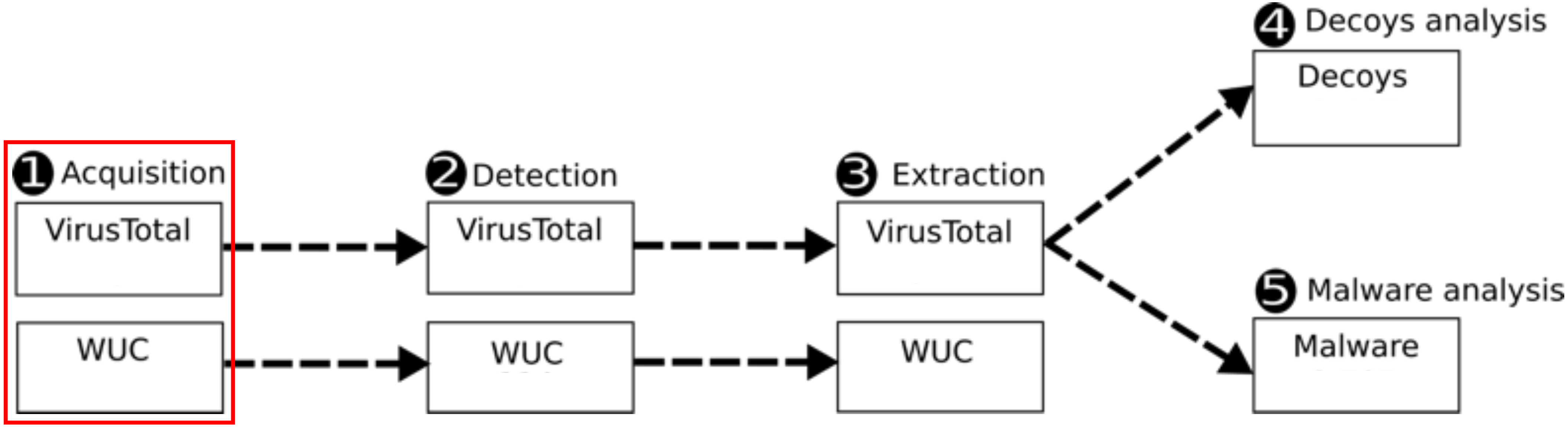
Exploit document infection process



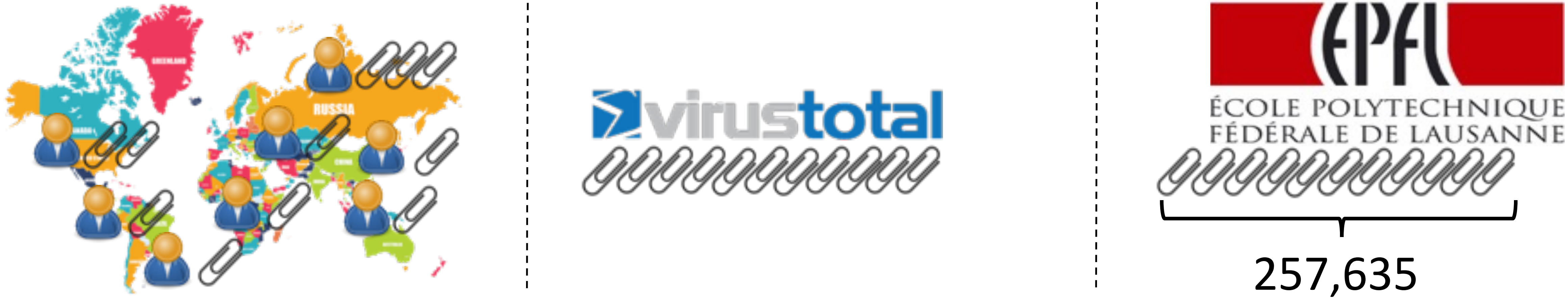
Data acquisition and processing workflow



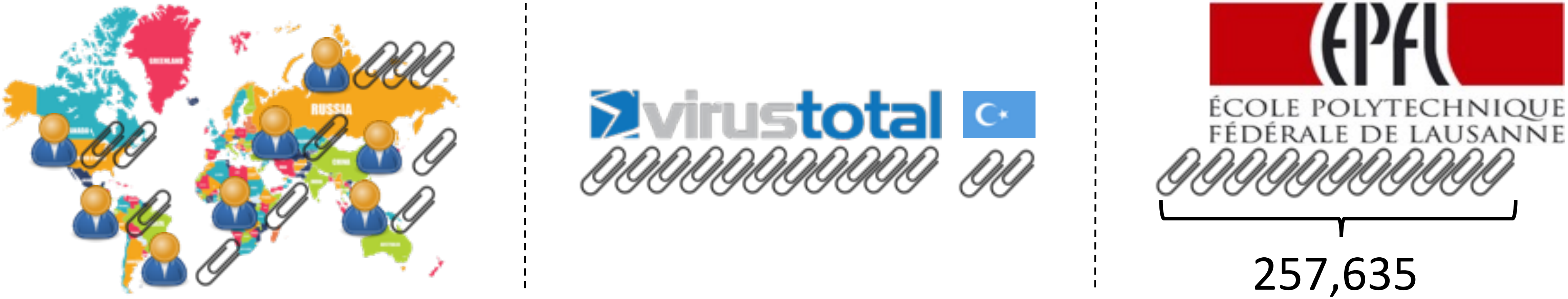
Data acquisition and processing workflow



Can we scale our analysis to hundreds of thousands of samples? Acquisition

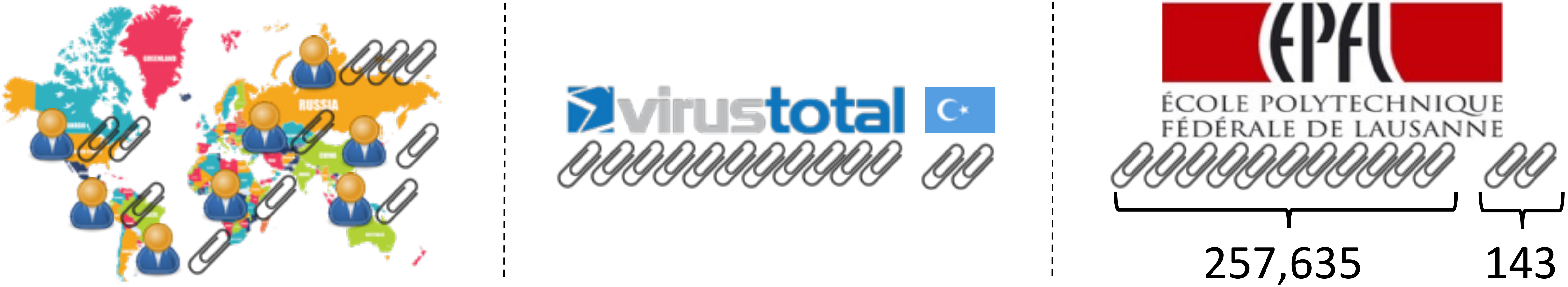


Can we scale our analysis to hundreds of thousands of samples? Acquisition



257,635

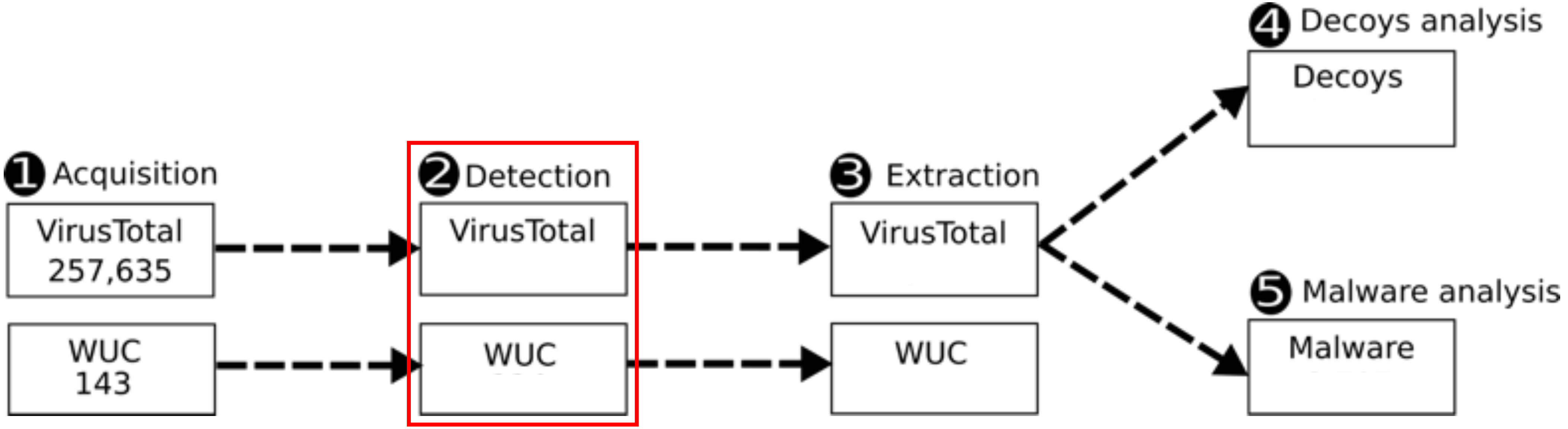
Can we scale our analysis to hundreds of thousands of samples? Acquisition



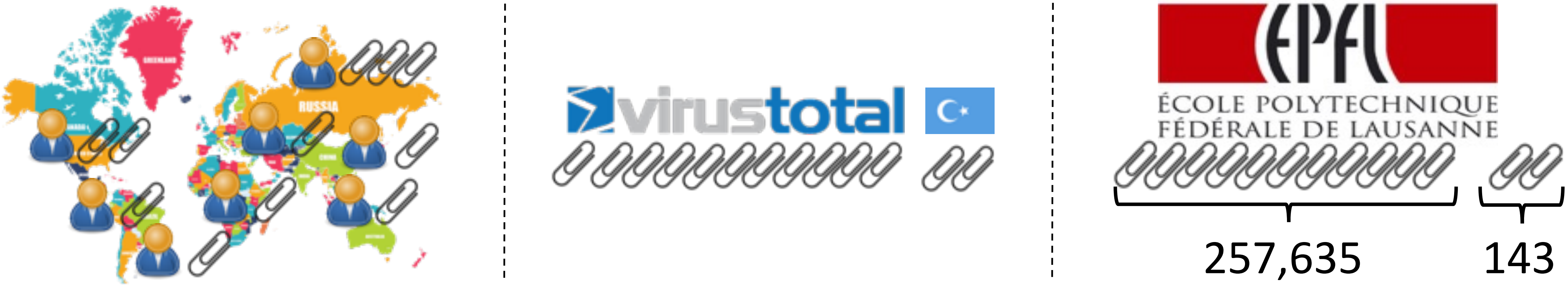
257,635

143

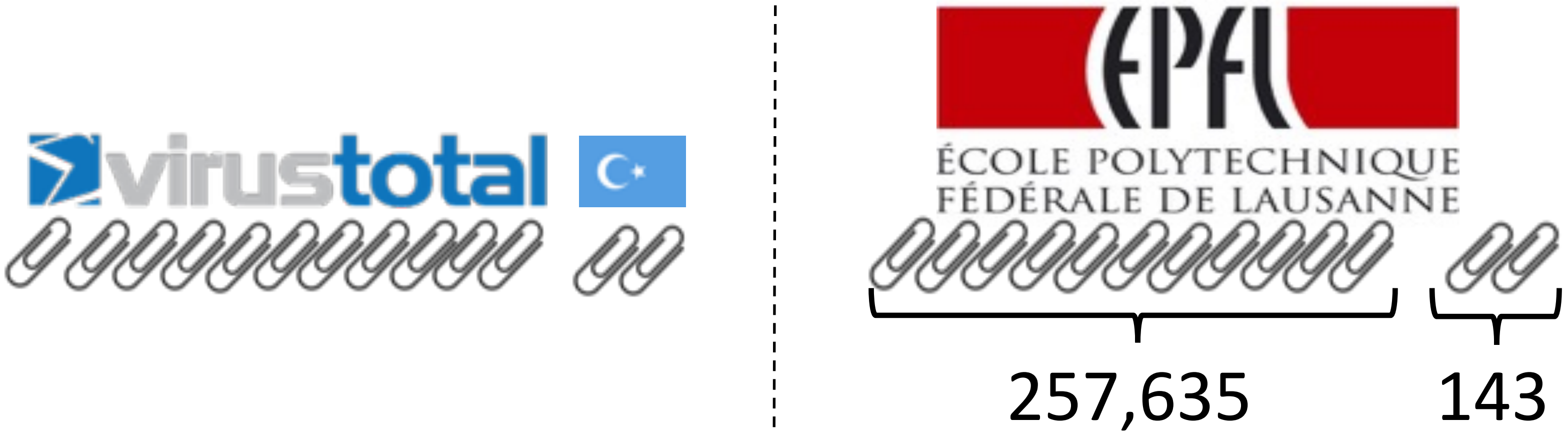
Data acquisition and processing workflow



Can we scale our analysis to hundreds of thousands of samples? Detection



Can we scale our analysis to hundreds of thousands of samples? Detection



257,635

143

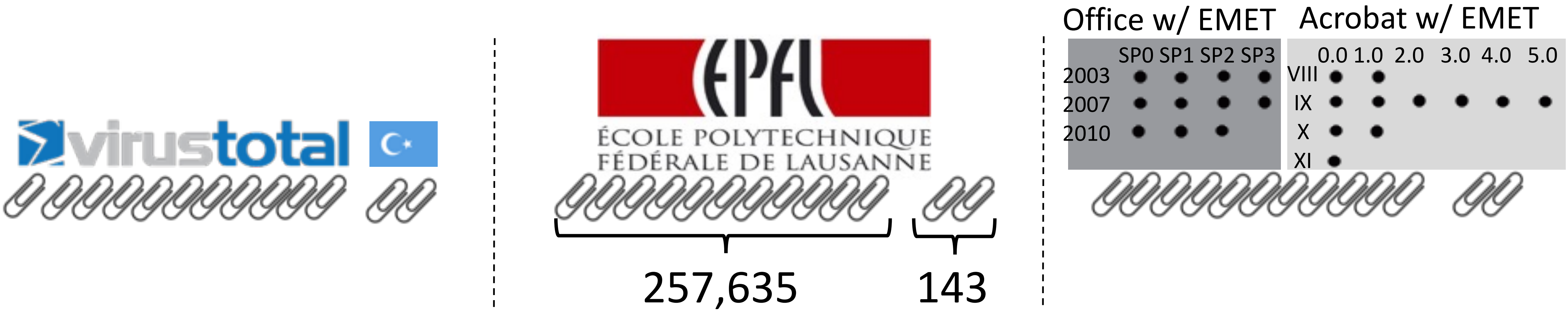
Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

Can we scale our analysis to hundreds of thousands of samples? Detection



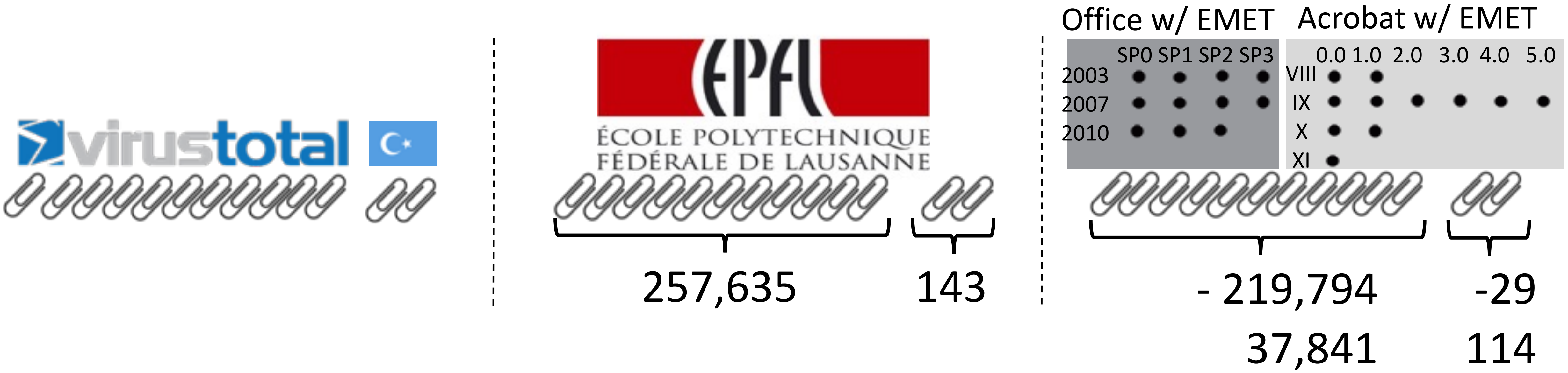
Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

Can we scale our analysis to hundreds of thousands of samples? Detection



Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

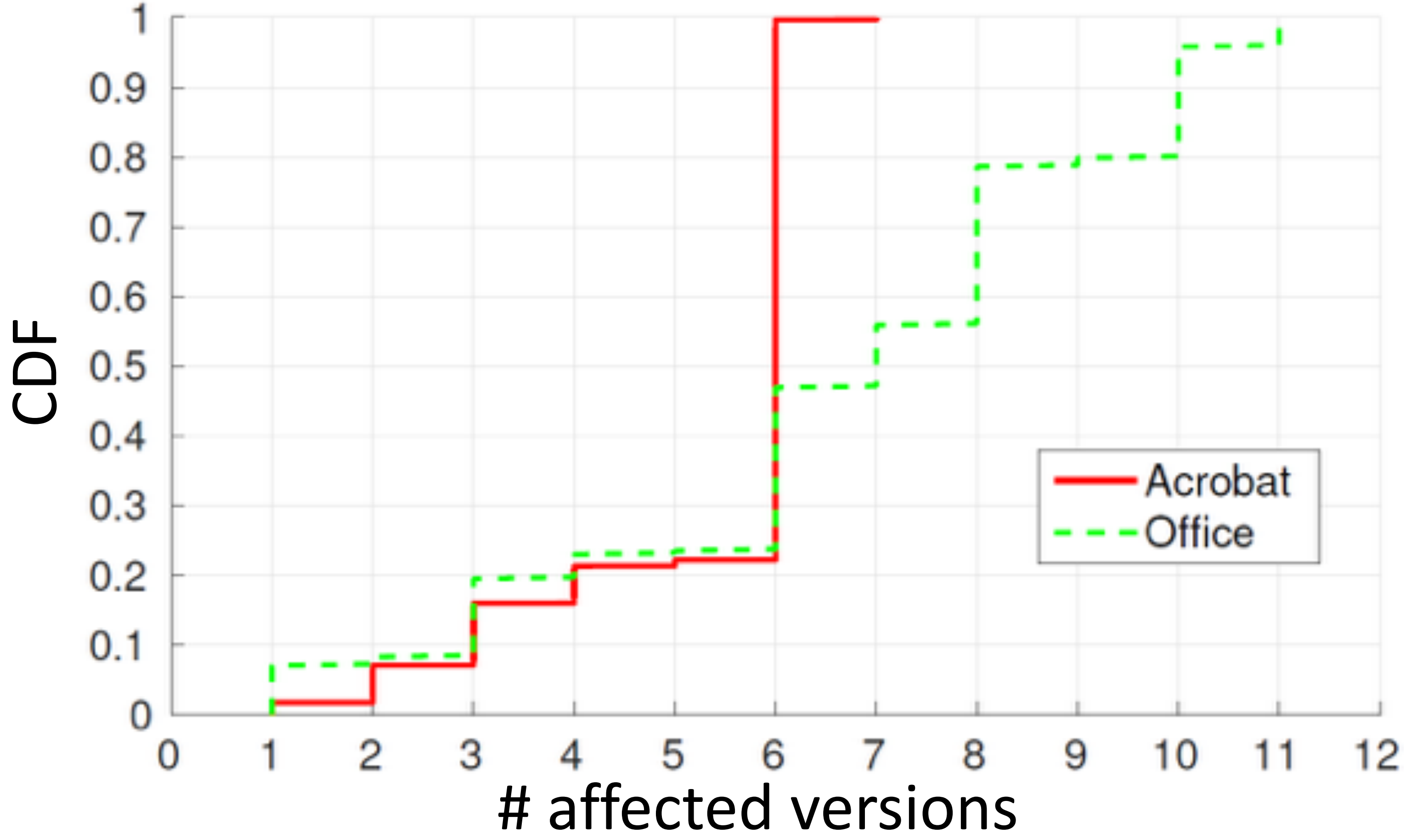
	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

257,635 143

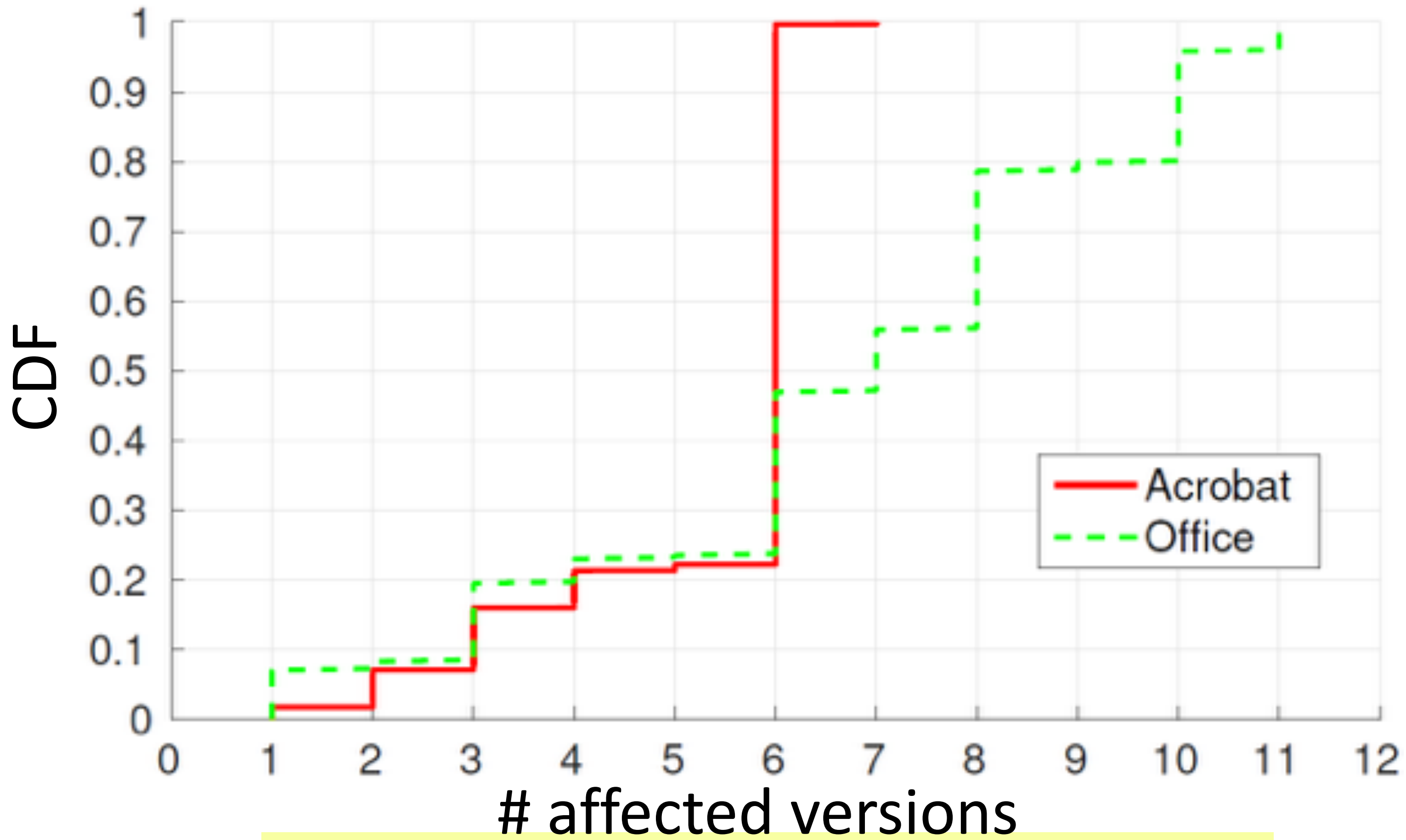
- 219,794 -29

37,841 114

How many versions of readers do we have to test?

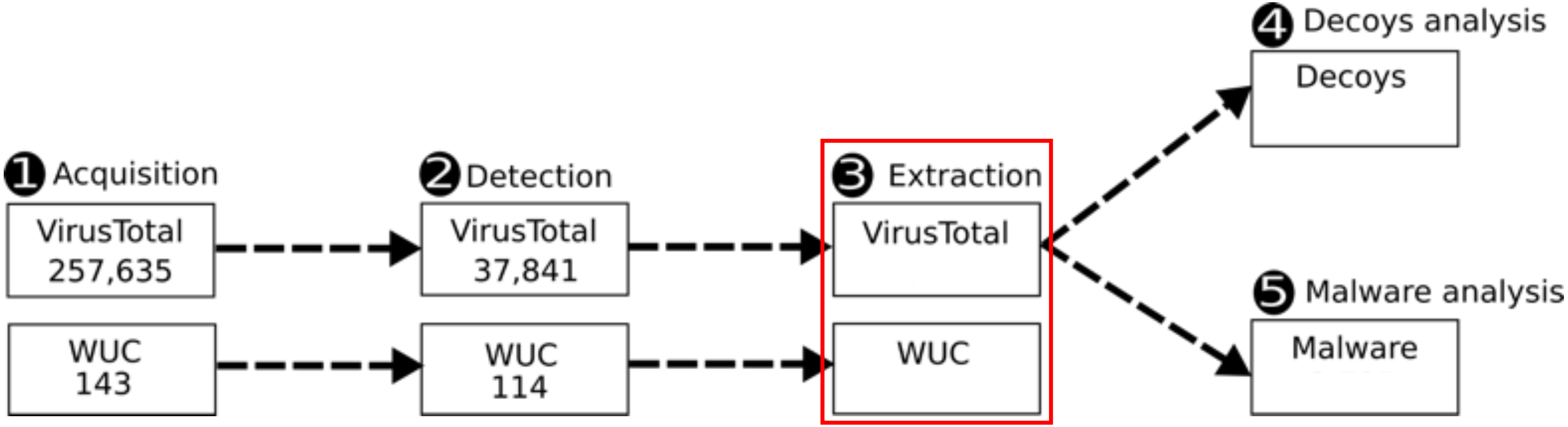


How many versions of readers do we have to test?



Few exploits are portable across all reader versions

Data acquisition and processing workflow



❶ Acquisition

VirusTotal 257,635

WUC 143

❷ Detection

VirusTotal 37,841

WUC 114

❸ Extraction

VirusTotal

WUC

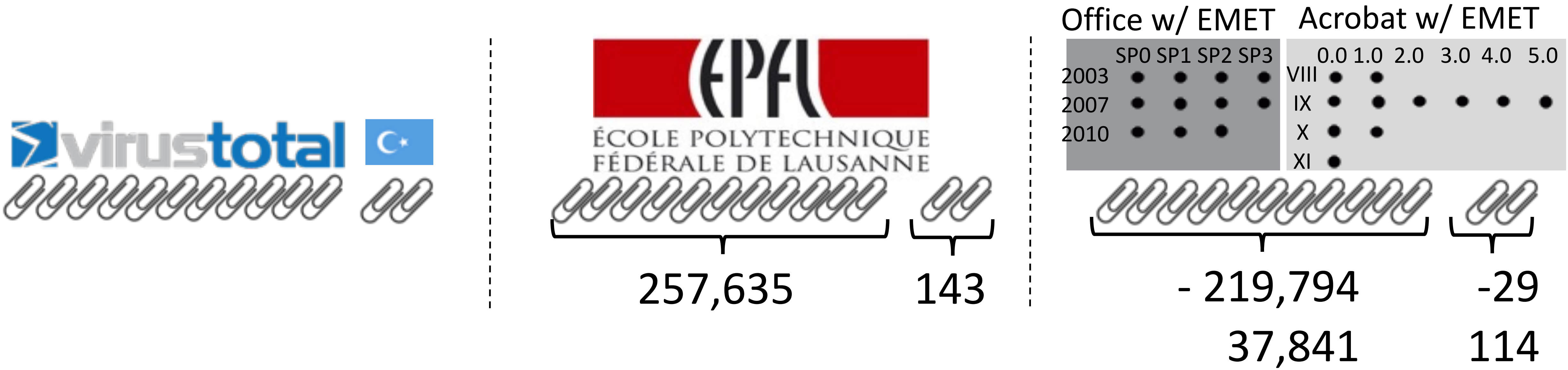
❹ Decoys analysis

Decoys

❺ Malware analysis

Malware

Can we scale our analysis to hundreds of thousands of samples? Extraction



Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

257,635 143

- 219,794 -29

37,841 114

Can we scale our analysis to hundreds of thousands of samples? Extraction

257,635

143

Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

- 219,794

-29

37,841

114

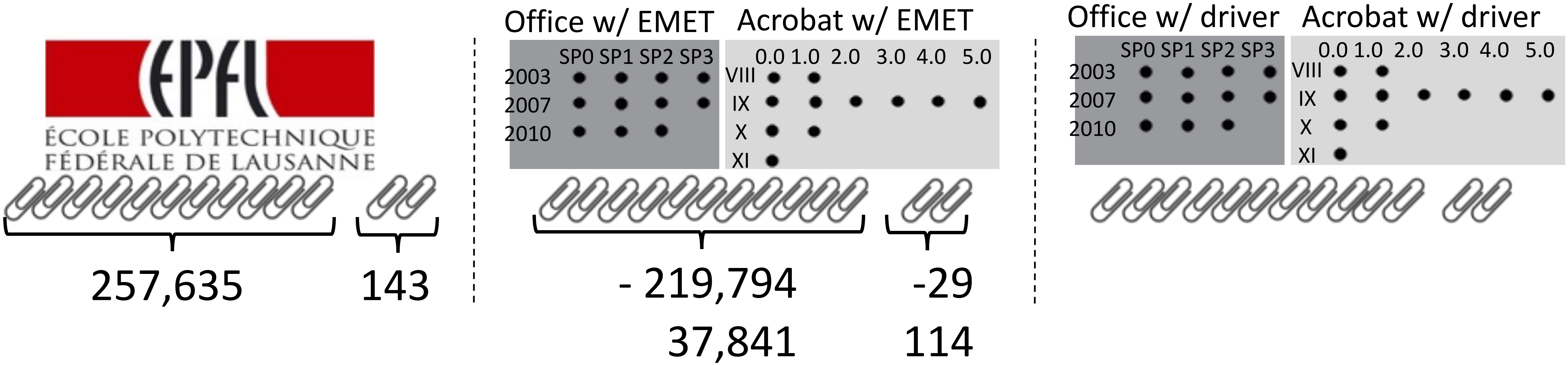
Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

Can we scale our analysis to hundreds of thousands of samples? Extraction



Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

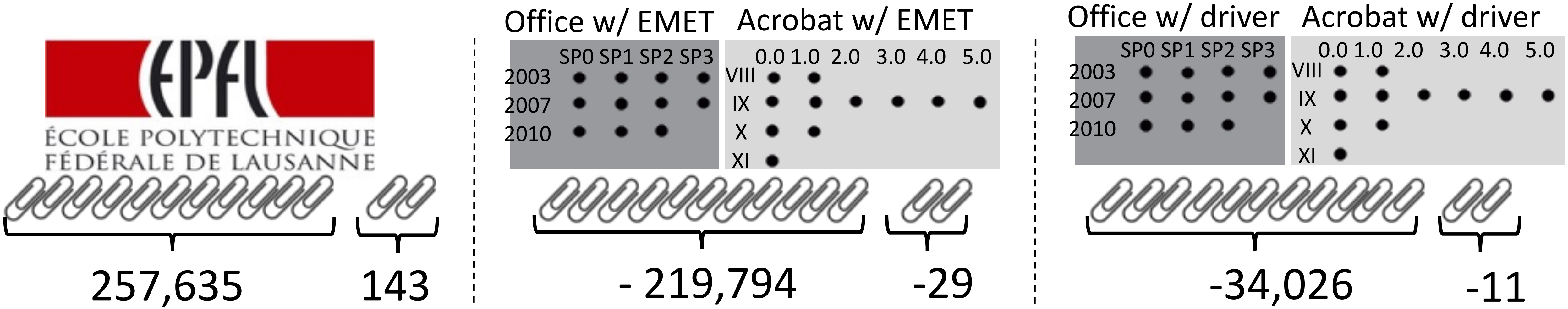
Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

Can we scale our analysis to hundreds of thousands of samples? Extraction



257,635 143

Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

- 219,794 -29

37,841 114

Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

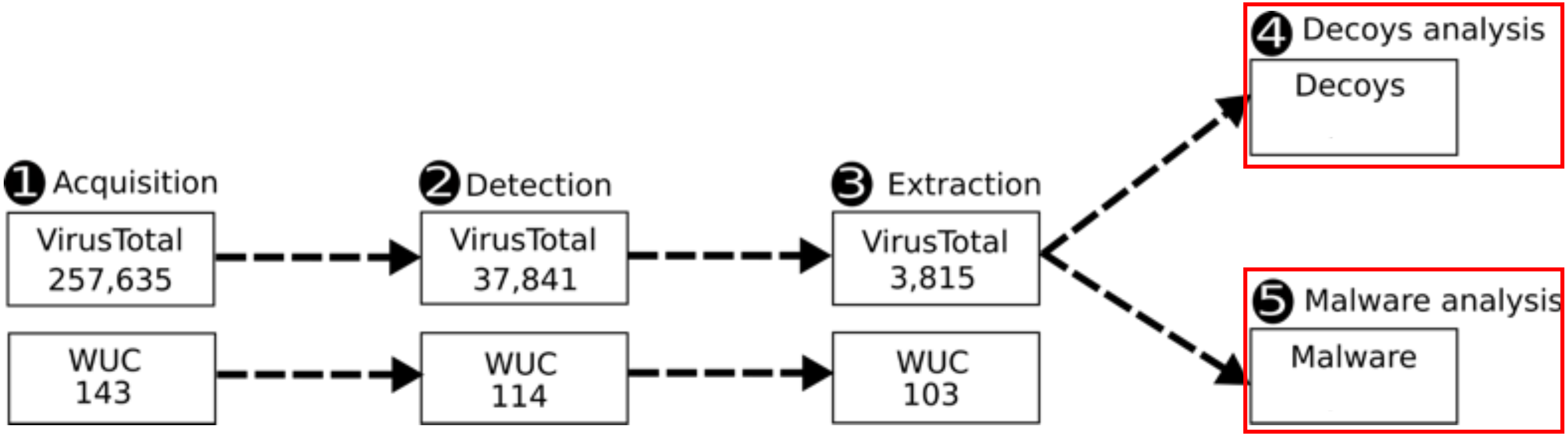
Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

-34,026 -11

3,815 103

Data acquisition and processing workflow



Can we scale our analysis to hundreds of thousands of samples? Analysis

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

257,635

143

Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

- 219,794

37,841

-29

114

Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

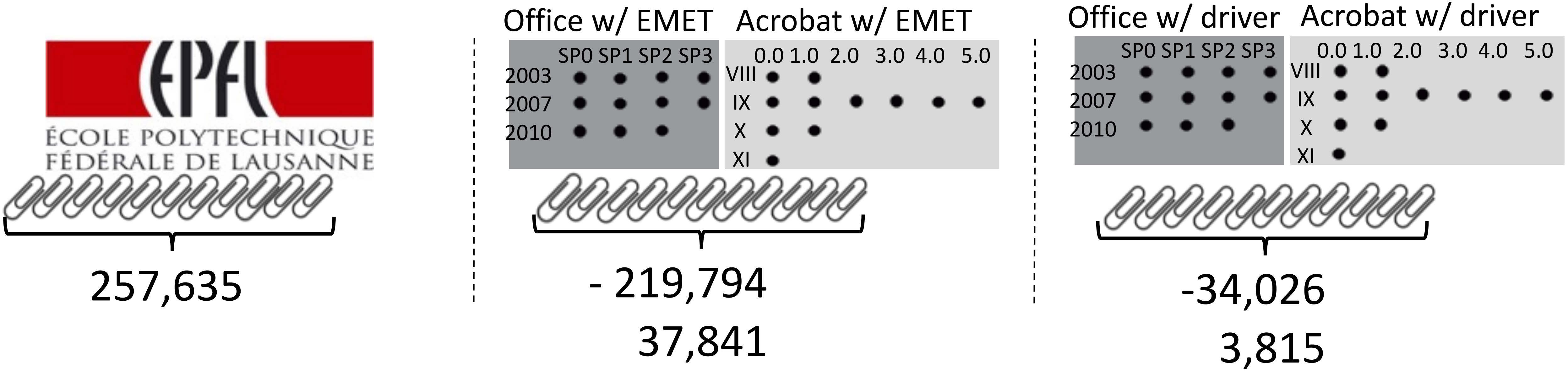
-34,026

3,815

-11

103

Can we scale our analysis to hundreds of thousands of samples? Analysis



ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

257,635

Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

- 219,794

37,841

Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

-34,026

3,815

Can we scale our analysis to hundreds of thousands of samples? Analysis

Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

- 219,794

37,841

Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

-34,026

3,815

Translators

Malware sandboxes

FireEye

Can we scale our analysis to hundreds of thousands of samples? Analysis

Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

- 219,794

37,841

Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

-34,026

3,815

Translators

Malware sandboxes

FireEye

Can we scale our analysis to hundreds of thousands of samples? Analysis

Office w/ EMET

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ EMET

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

- 219,794

37,841

Office w/ driver

	SP0	SP1	SP2	SP3
2003	●	●	●	●
2007	●	●	●	●
2010	●	●	●	

Acrobat w/ driver

	0.0	1.0	2.0	3.0	4.0	5.0
VIII	●	●				
IX	●	●	●	●	●	●
X	●	●				
XI	●					

-34,026

3,815

Translators

2,447

Malware sandboxes

FireEye

3,705

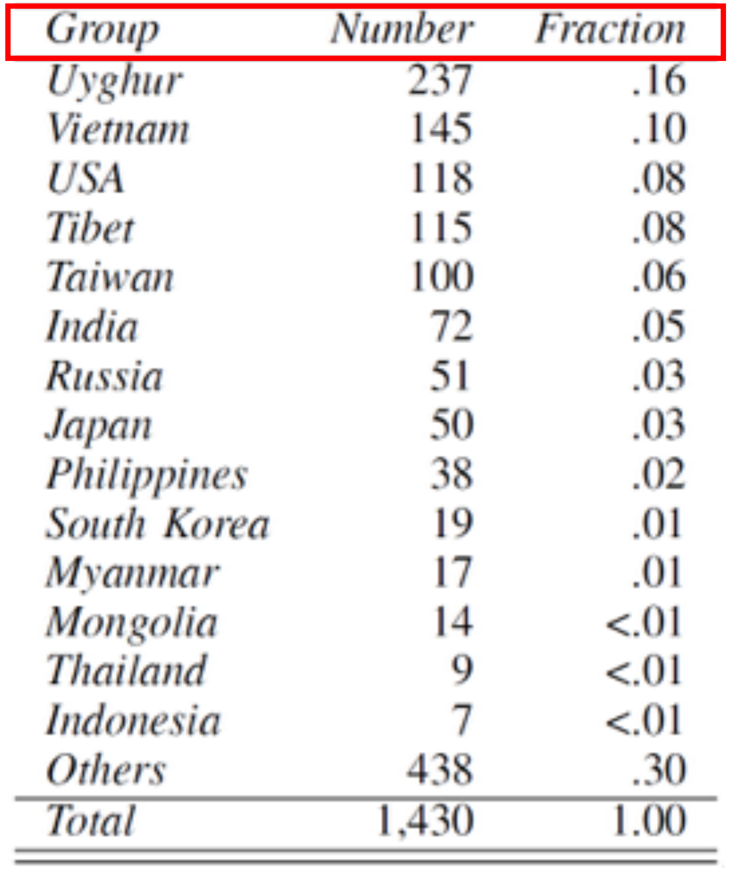
Outline

1) Methodology

2) Analysis of exploit documents

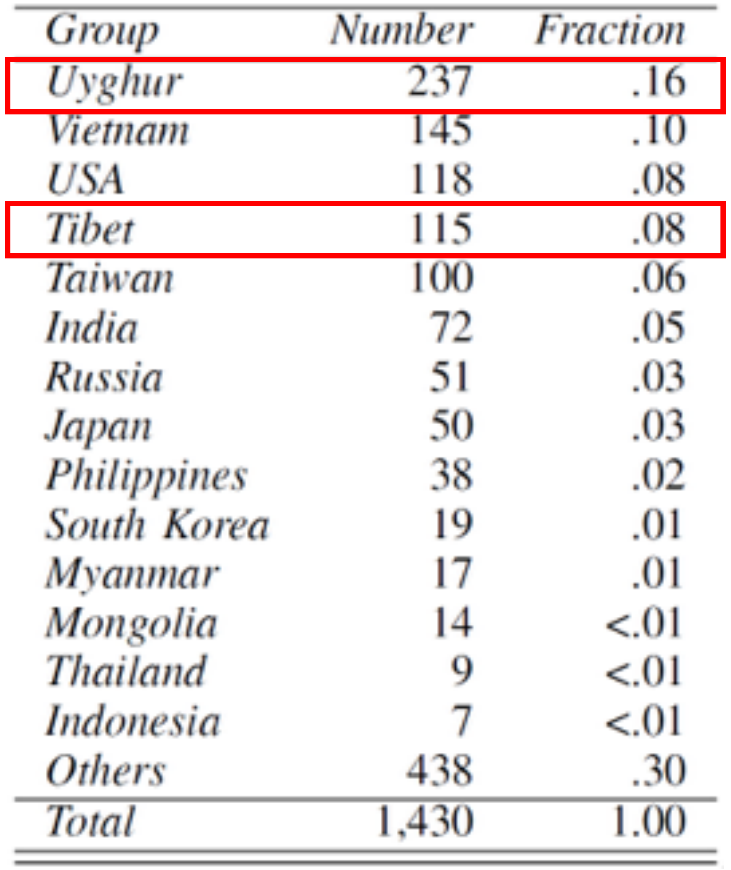
3) Future work

Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)



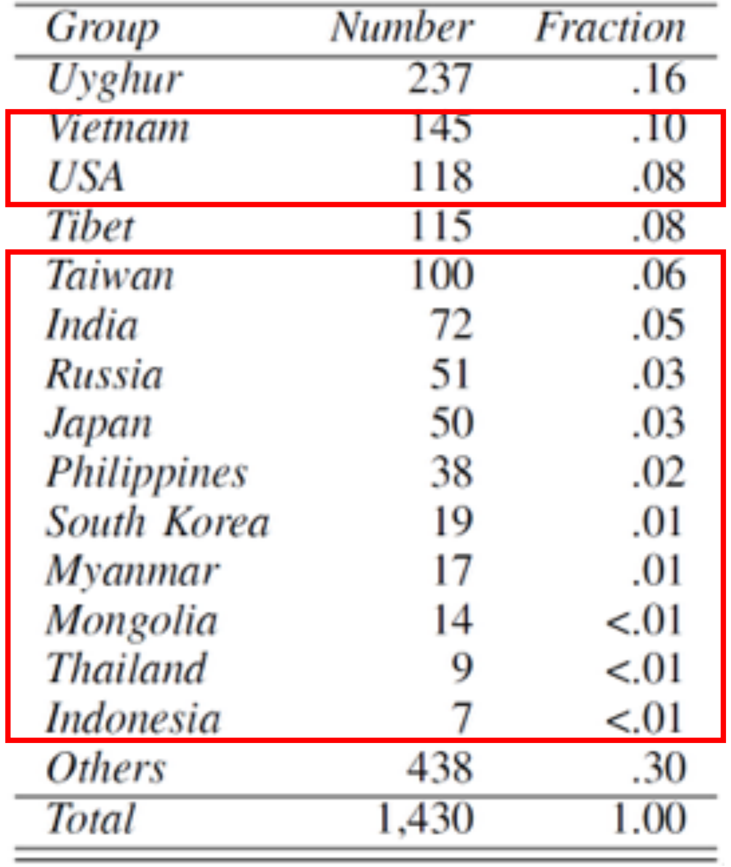
Group	*Number*	*Fraction*
Uyghur	237	.16
Vietnam	145	.10
USA	118	.08
Tibet	115	.08
Taiwan	100	.06
India	72	.05
Russia	51	.03
Japan	50	.03
Philippines	38	.02
South Korea	19	.01
Myanmar	17	.01
Mongolia	14	<.01
Thailand	9	<.01
Indonesia	7	<.01
Others	438	.30
Total	1,430	1.00

Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)



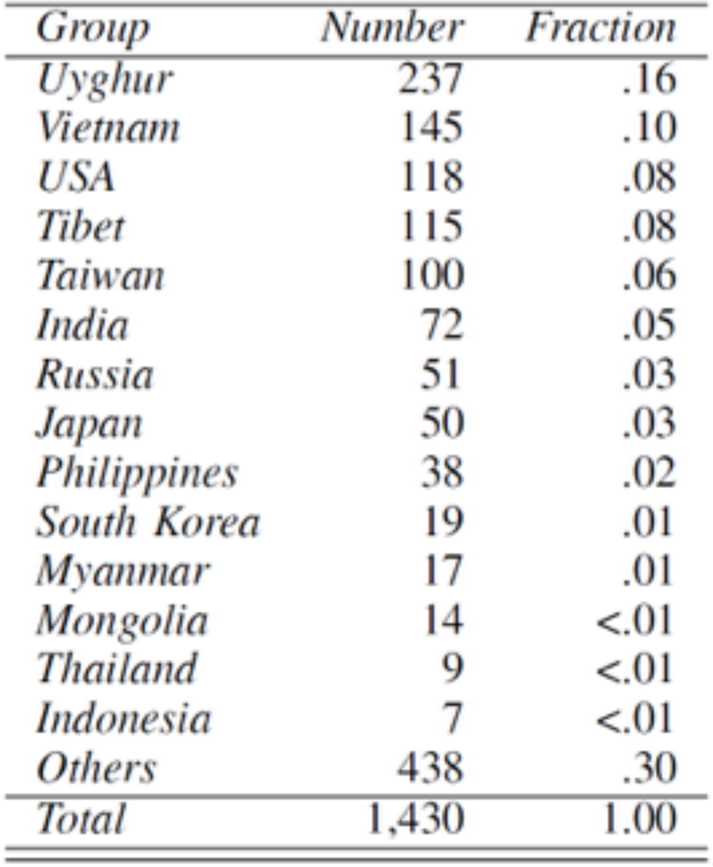
Group	*Number*	*Fraction*
Uyghur	237	.16
Vietnam	145	.10
USA	118	.08
Tibet	115	.08
Taiwan	100	.06
India	72	.05
Russia	51	.03
Japan	50	.03
Philippines	38	.02
South Korea	19	.01
Myanmar	17	.01
Mongolia	14	<.01
Thailand	9	<.01
Indonesia	7	<.01
Others	438	.30
Total	1,430	1.00

Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)



Group	*Number*	*Fraction*
Uyghur	237	.16
Vietnam	145	.10
USA	118	.08
Tibet	115	.08
Taiwan	100	.06
India	72	.05
Russia	51	.03
Japan	50	.03
Philippines	38	.02
South Korea	19	.01
Myanmar	17	.01
Mongolia	14	<.01
Thailand	9	<.01
Indonesia	7	<.01
Others	438	.30
Total	1,430	1.00

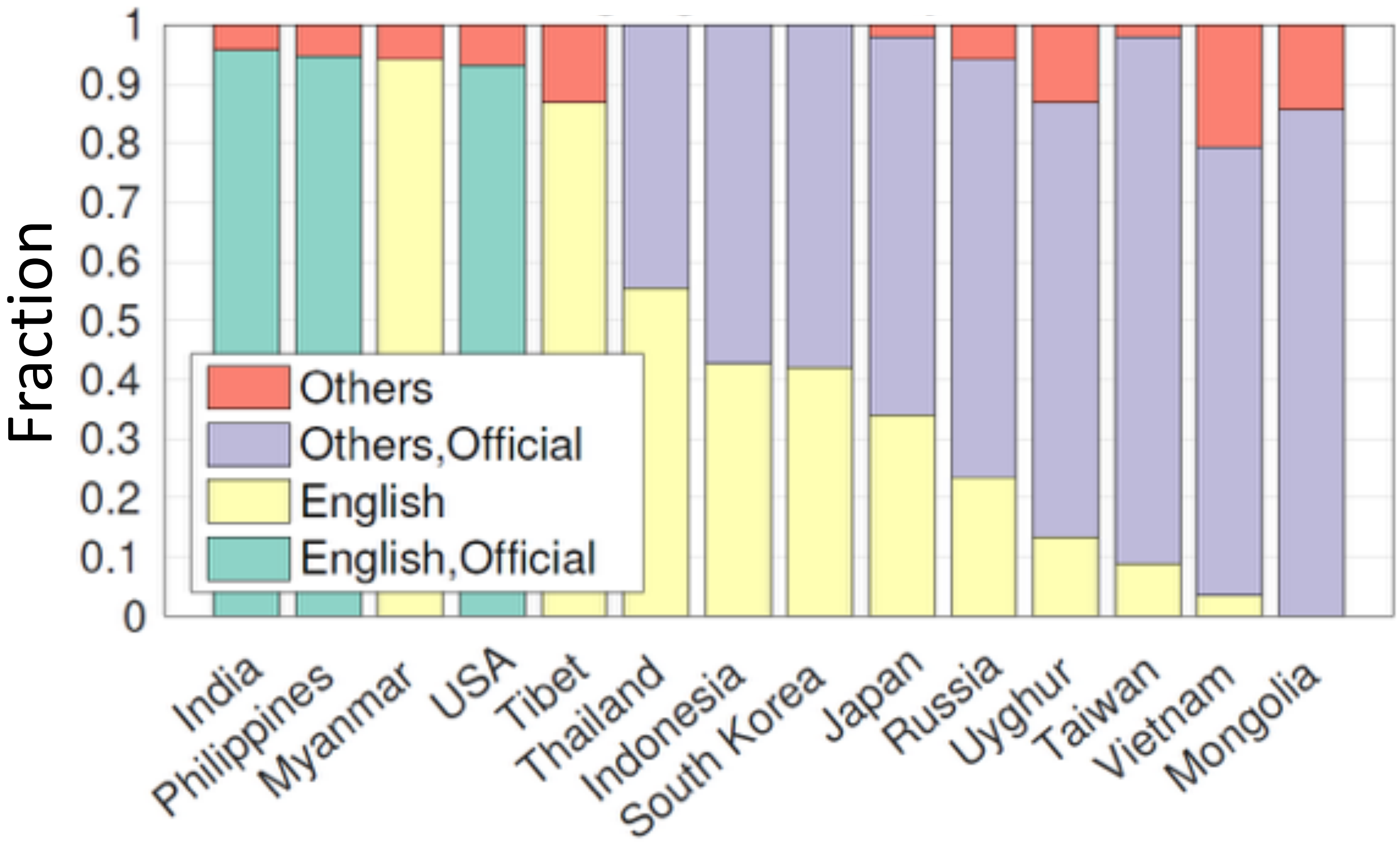
Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)



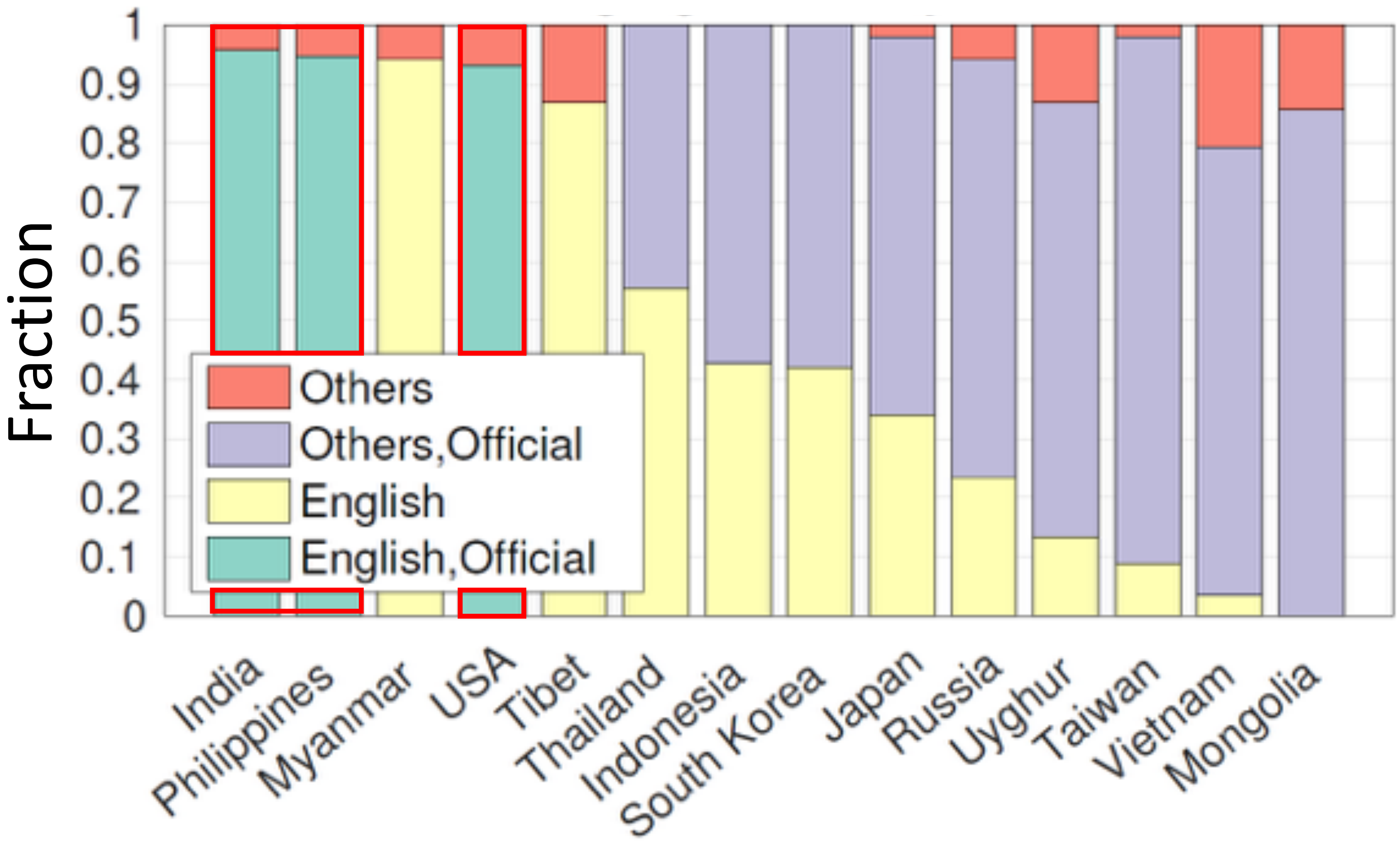
Group	*Number*	*Fraction*
Uyghur	237	.16
Vietnam	145	.10
USA	118	.08
Tibet	115	.08
Taiwan	100	.06
India	72	.05
Russia	51	.03
Japan	50	.03
Philippines	38	.02
South Korea	19	.01
Myanmar	17	.01
Mongolia	14	<.01
Thailand	9	<.01
Indonesia	7	<.01
Others	438	.30
Total	1,430	1.00

VirusTotal gives visibility into attacks targeting numerous groups

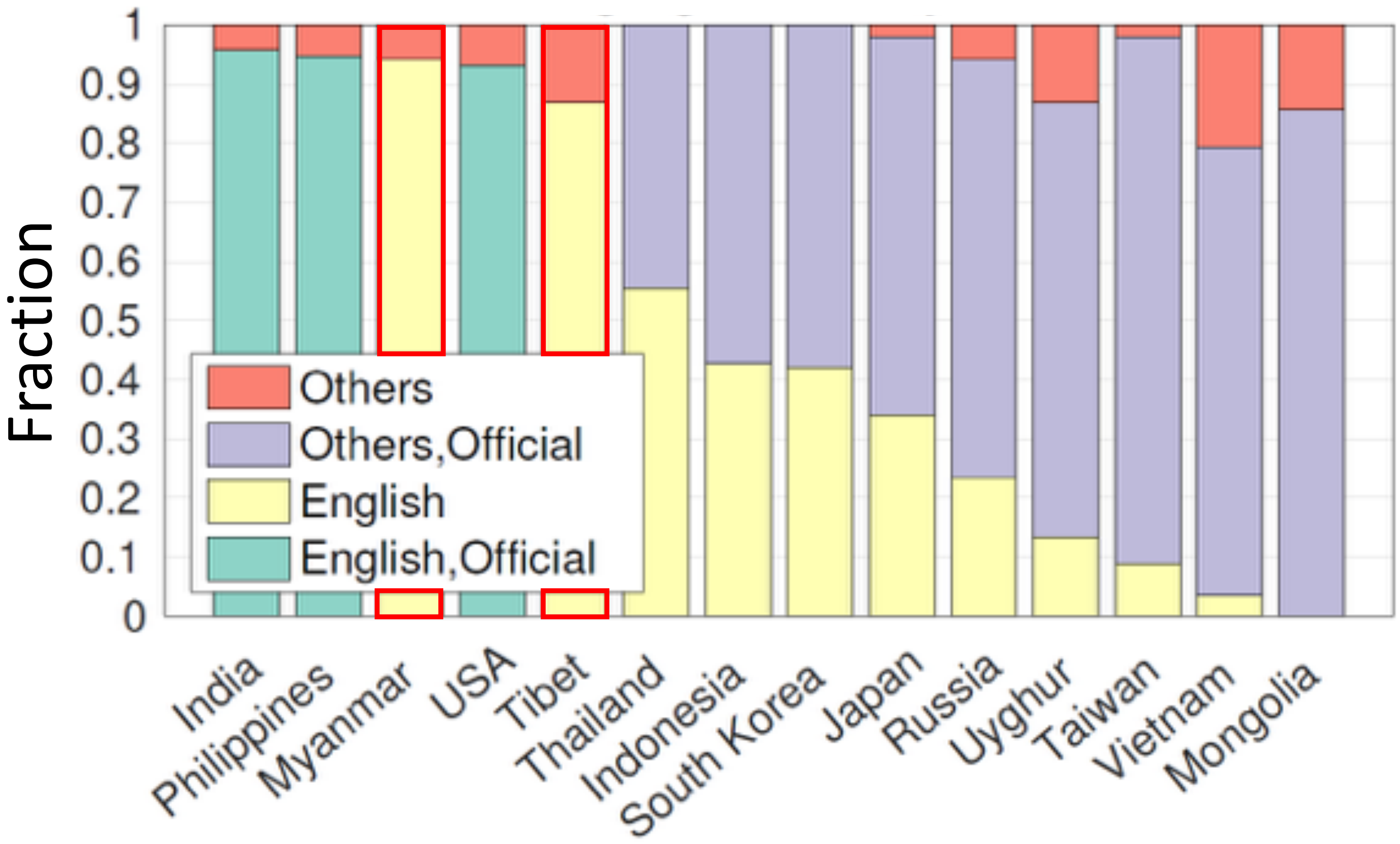
How attacks faced by different groups compare with each other? Languages of decoys



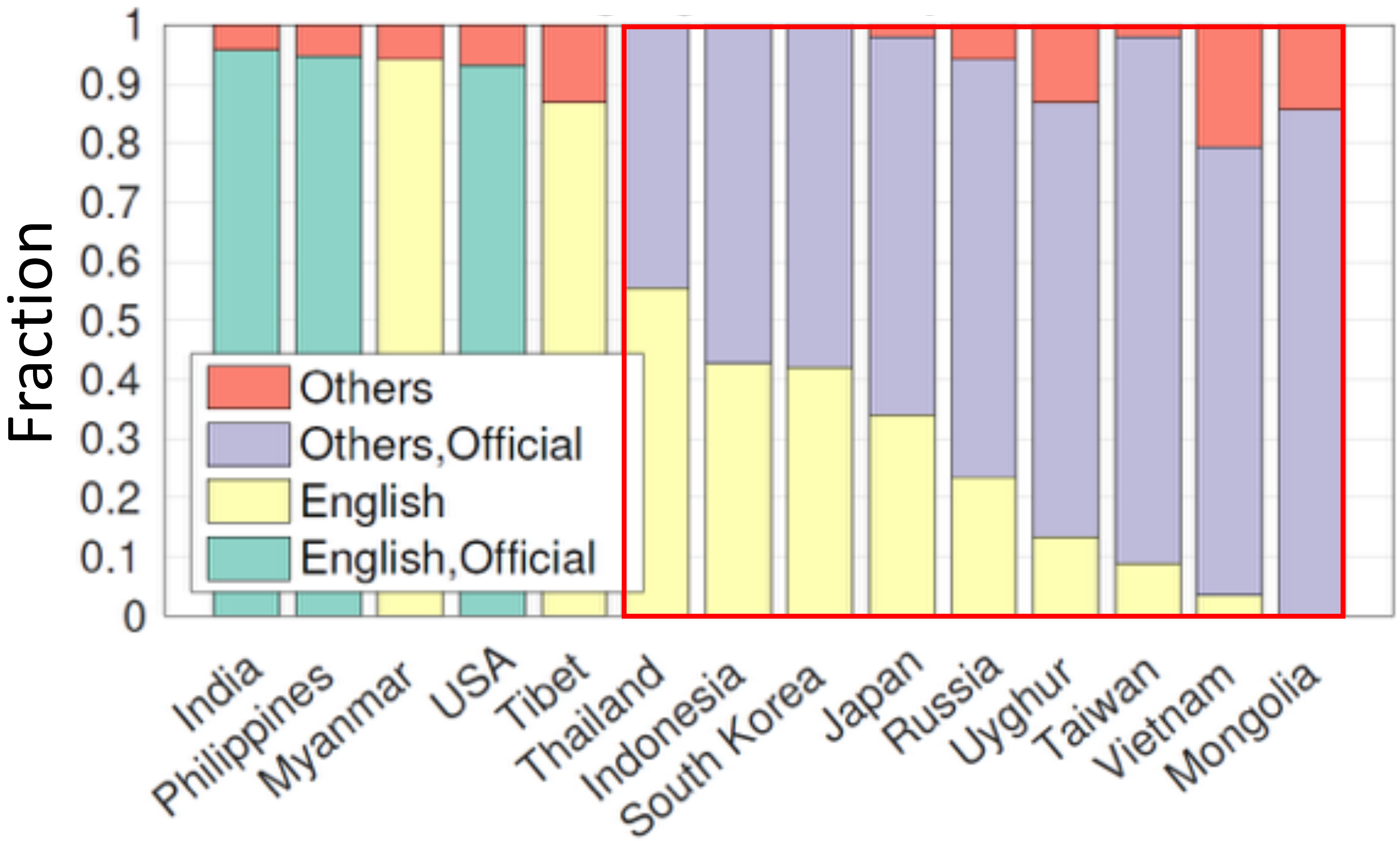
How attacks faced by different groups compare with each other? Languages of decoys



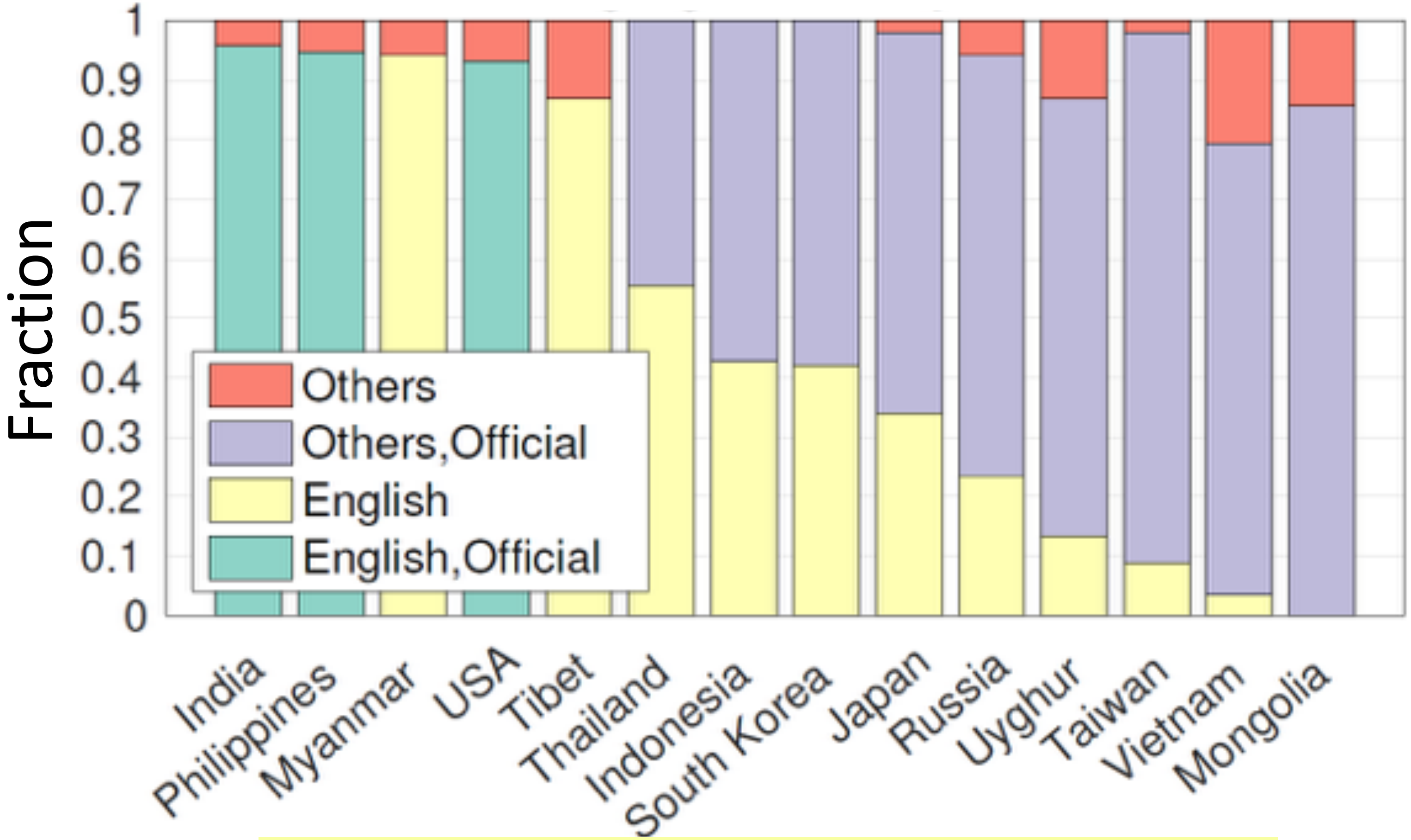
How attacks faced by different groups compare with each other? Languages of decoys



How attacks faced by different groups compare with each other? Languages of decoys

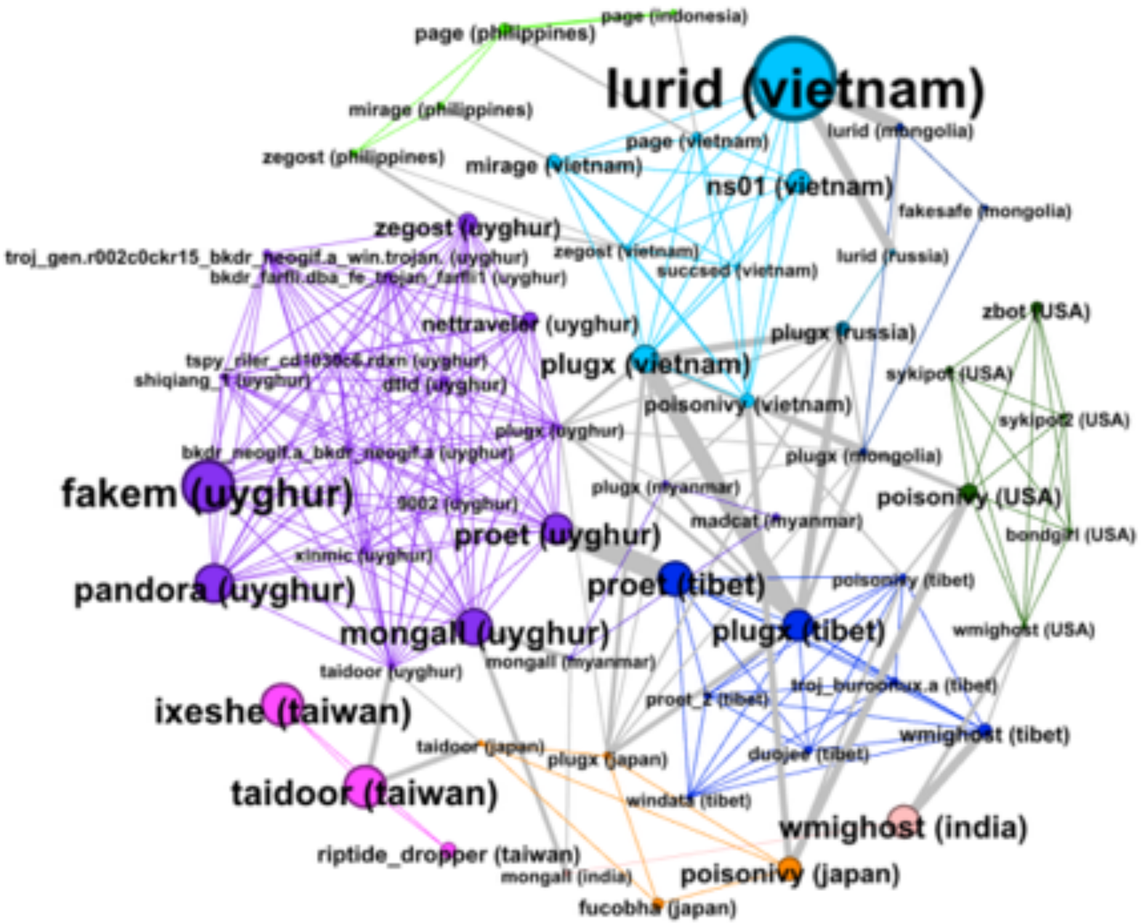


How attacks faced by different groups compare with each other? Languages of decoys

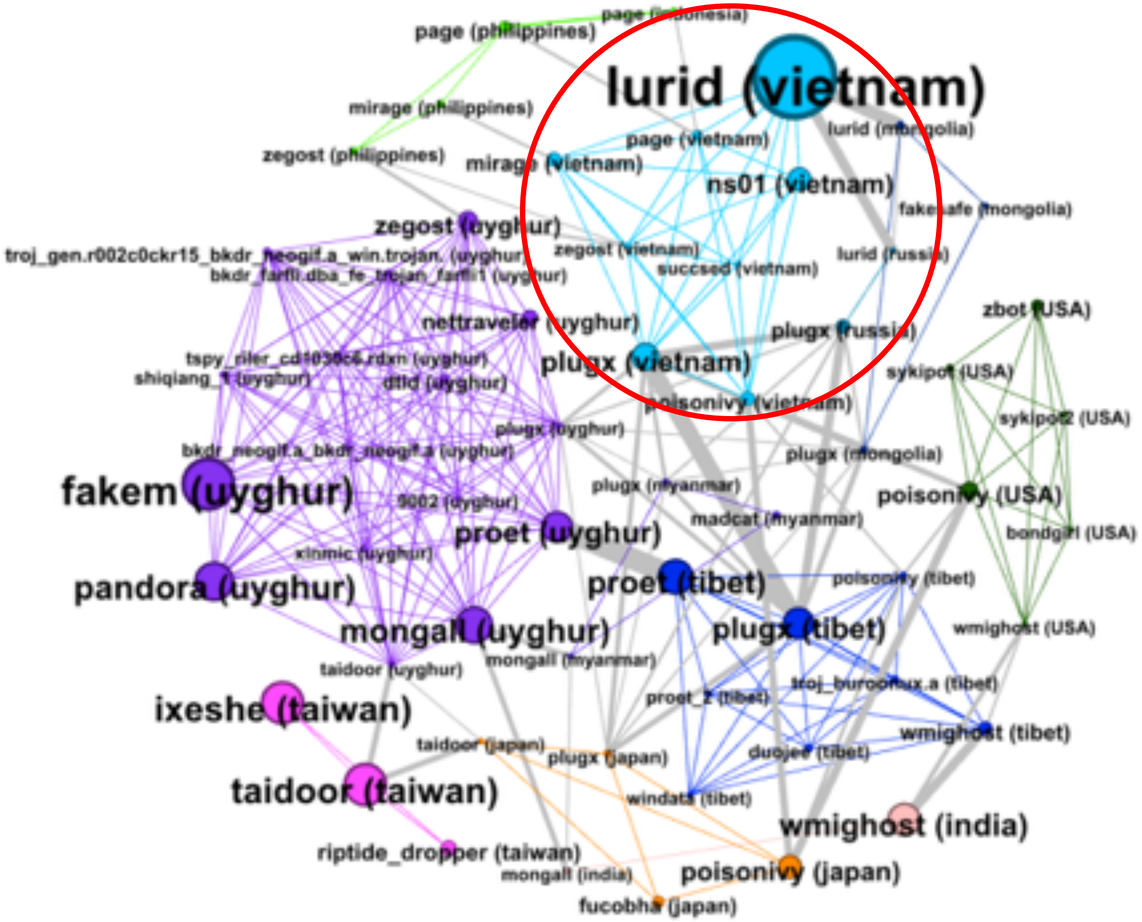


Decoys tend to use the official language of the groups they target

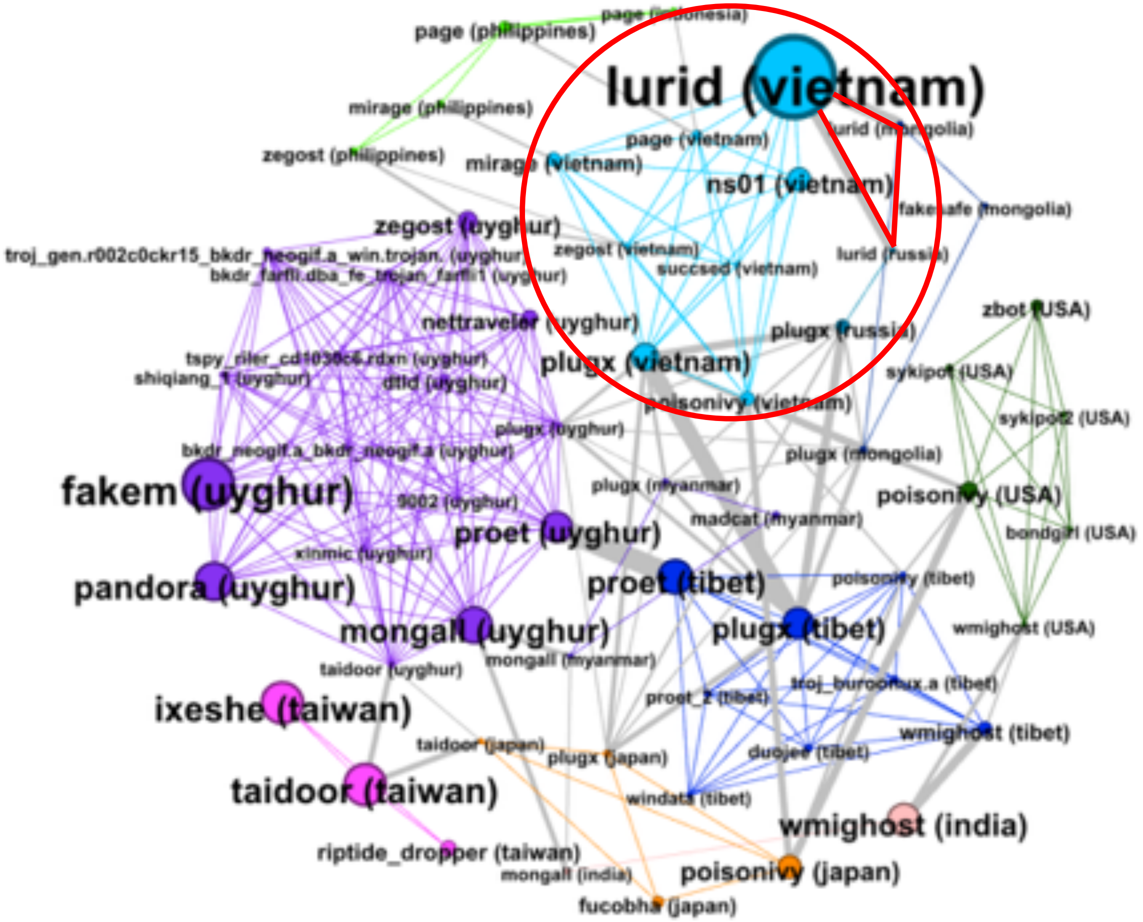
How attacks faced by different groups compare with each other? Malware targeting



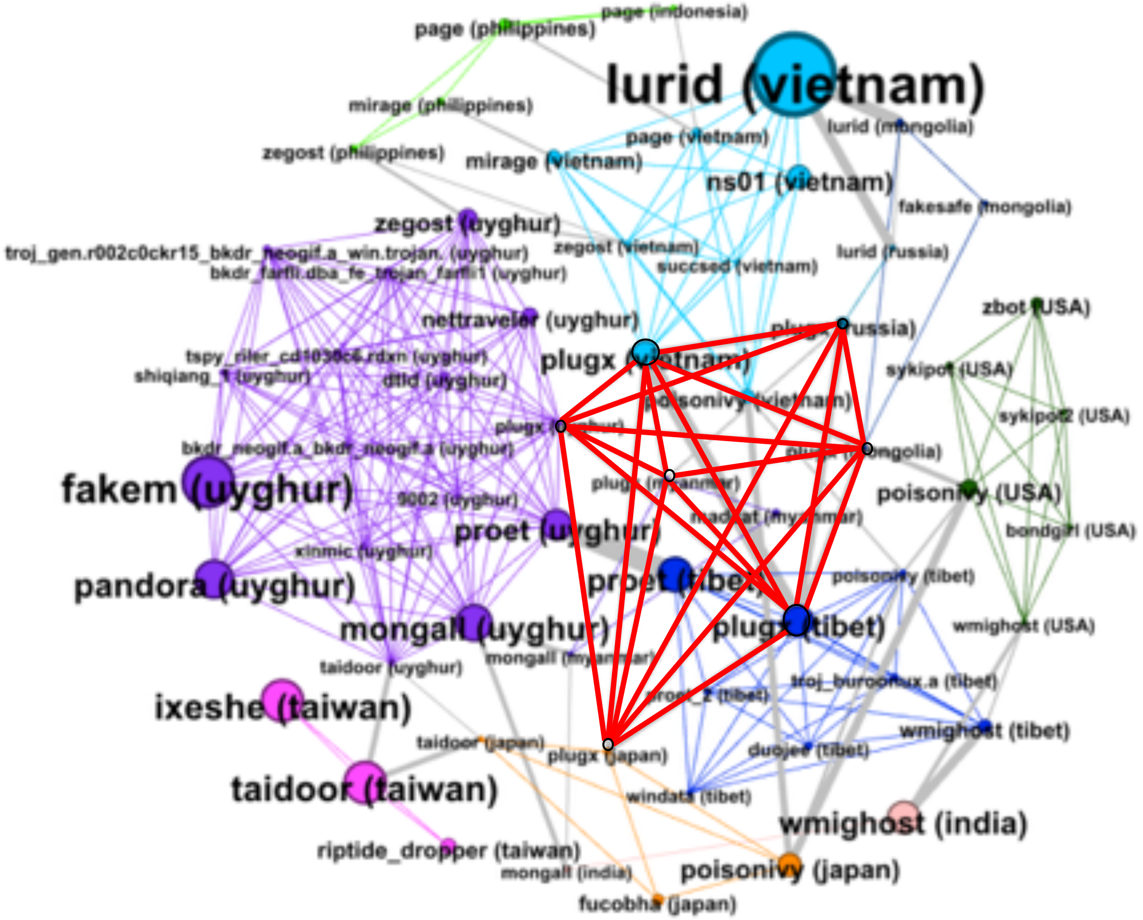
How attacks faced by different groups compare with each other? Malware targeting



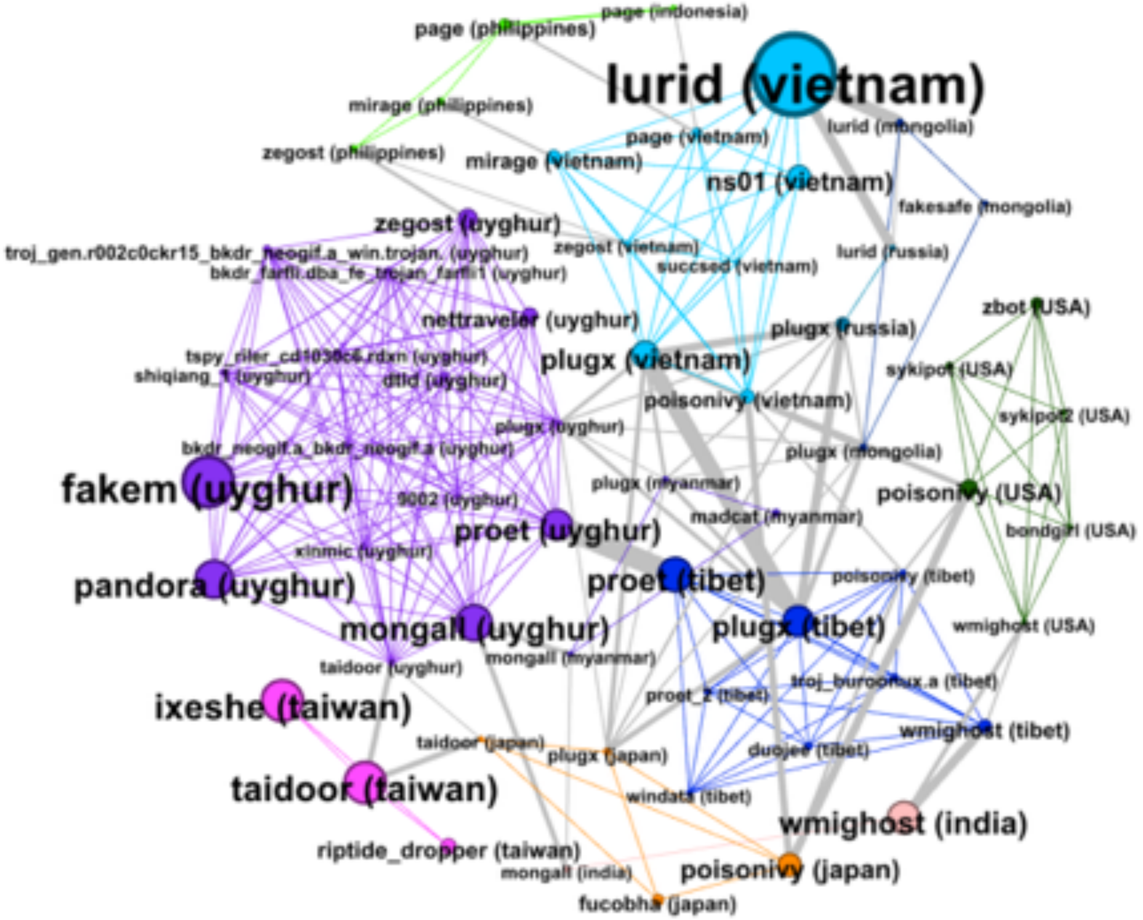
How attacks faced by different groups compare with each other? Malware targeting



How attacks faced by different groups compare with each other? Malware targeting



How attacks faced by different groups compare with each other? Malware targeting

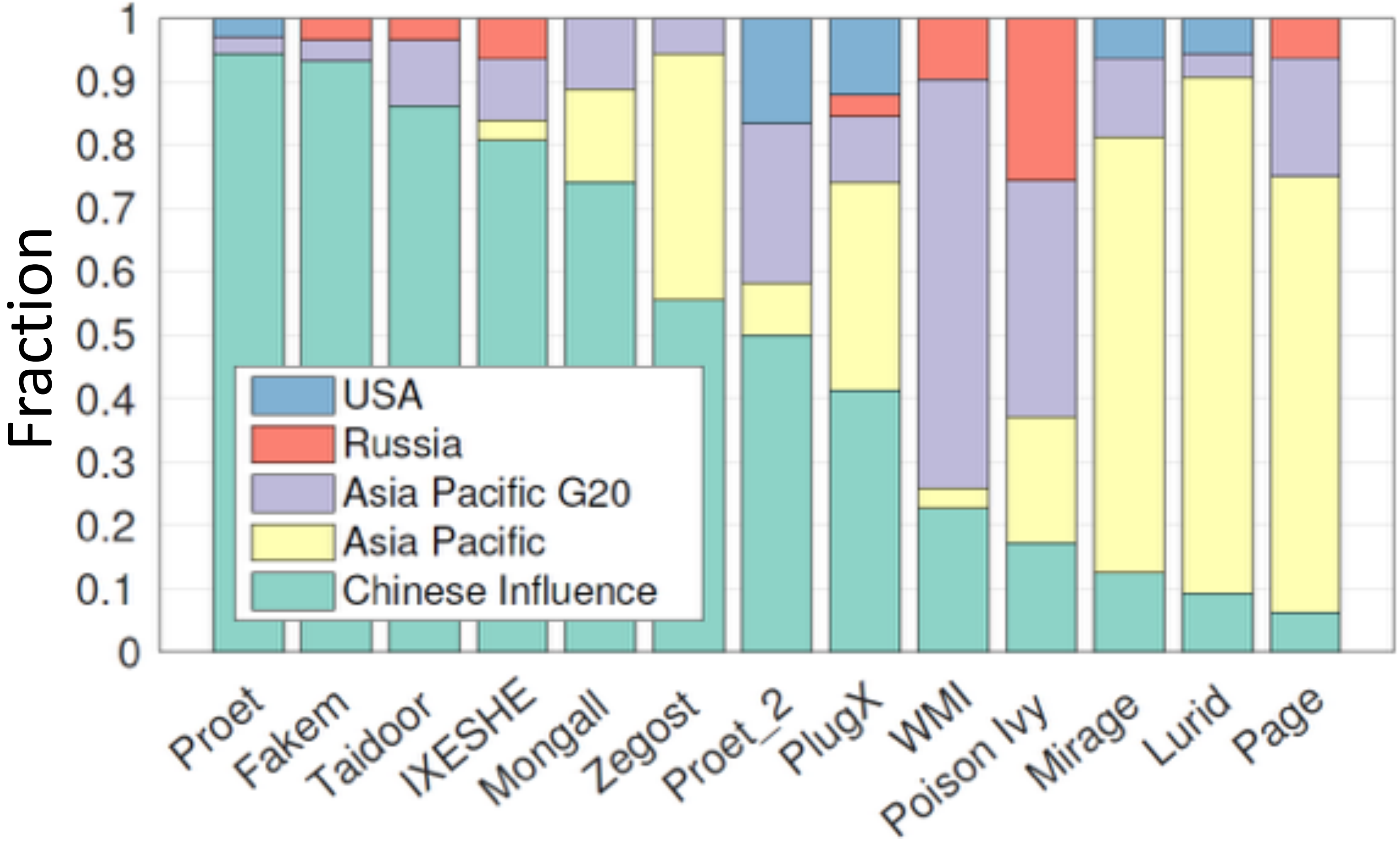


From our dataset, malware families tend to target one or two countries

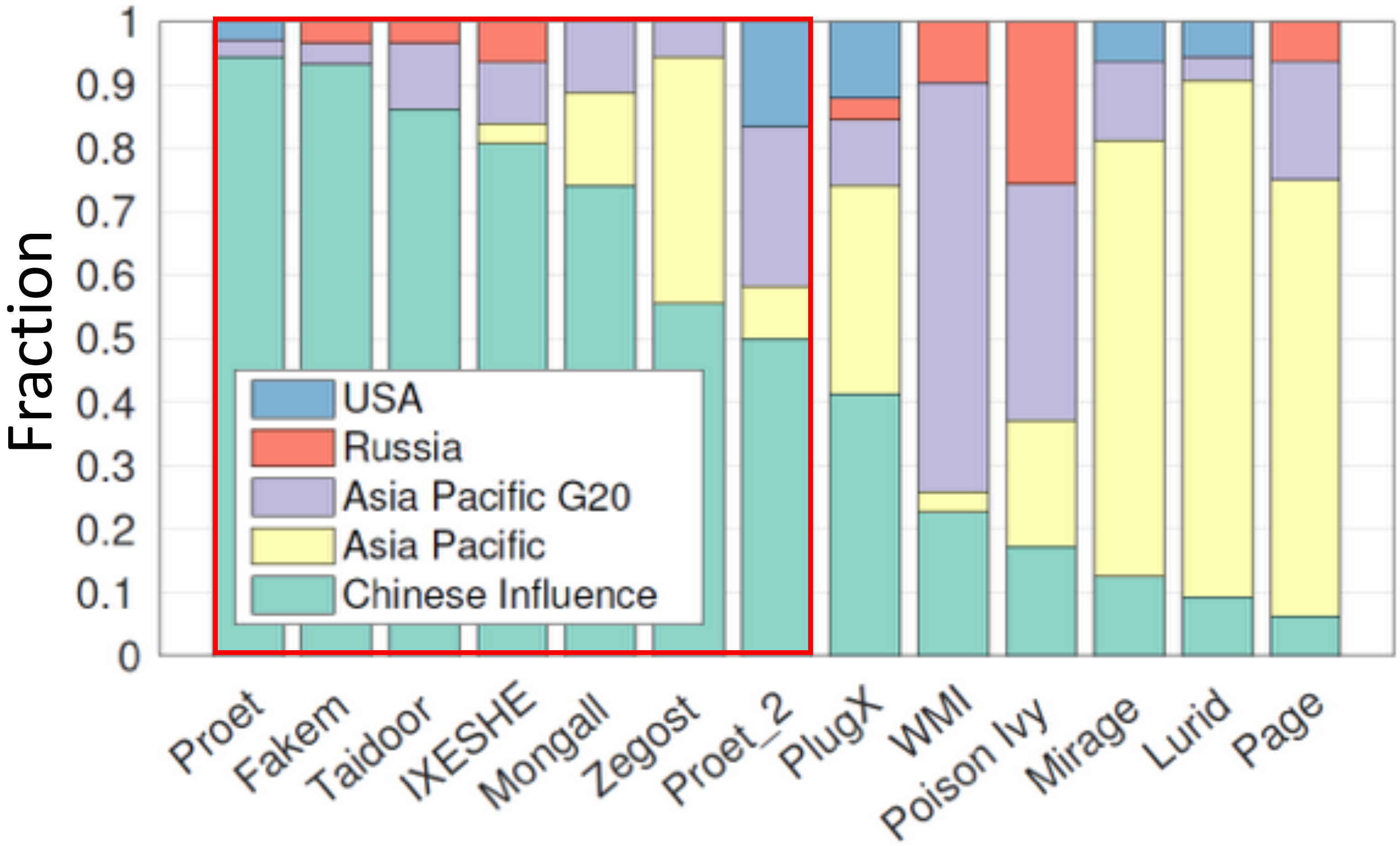
Targeted regions

- Chinese influence: Tibet, Uyghur, Taiwan
- Asia Pacific: Myanmar, the Philippines, Thailand, and Vietnam
- Asia Pacific, G20: India, Indonesia, Japan, and South Korea
- Russia and USA

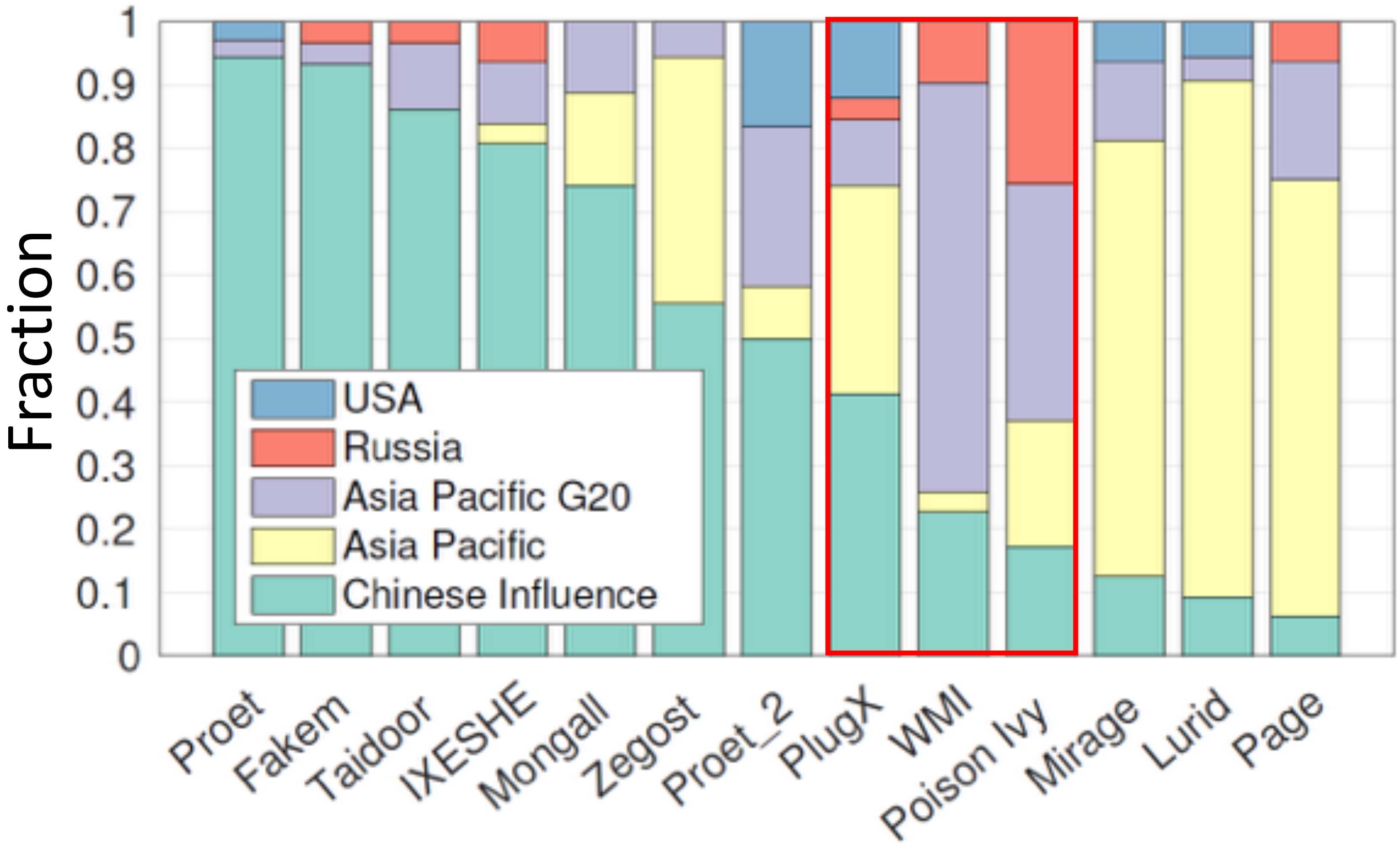
How do attacks faced by different groups compare with each other? Malware targeting (cont.)



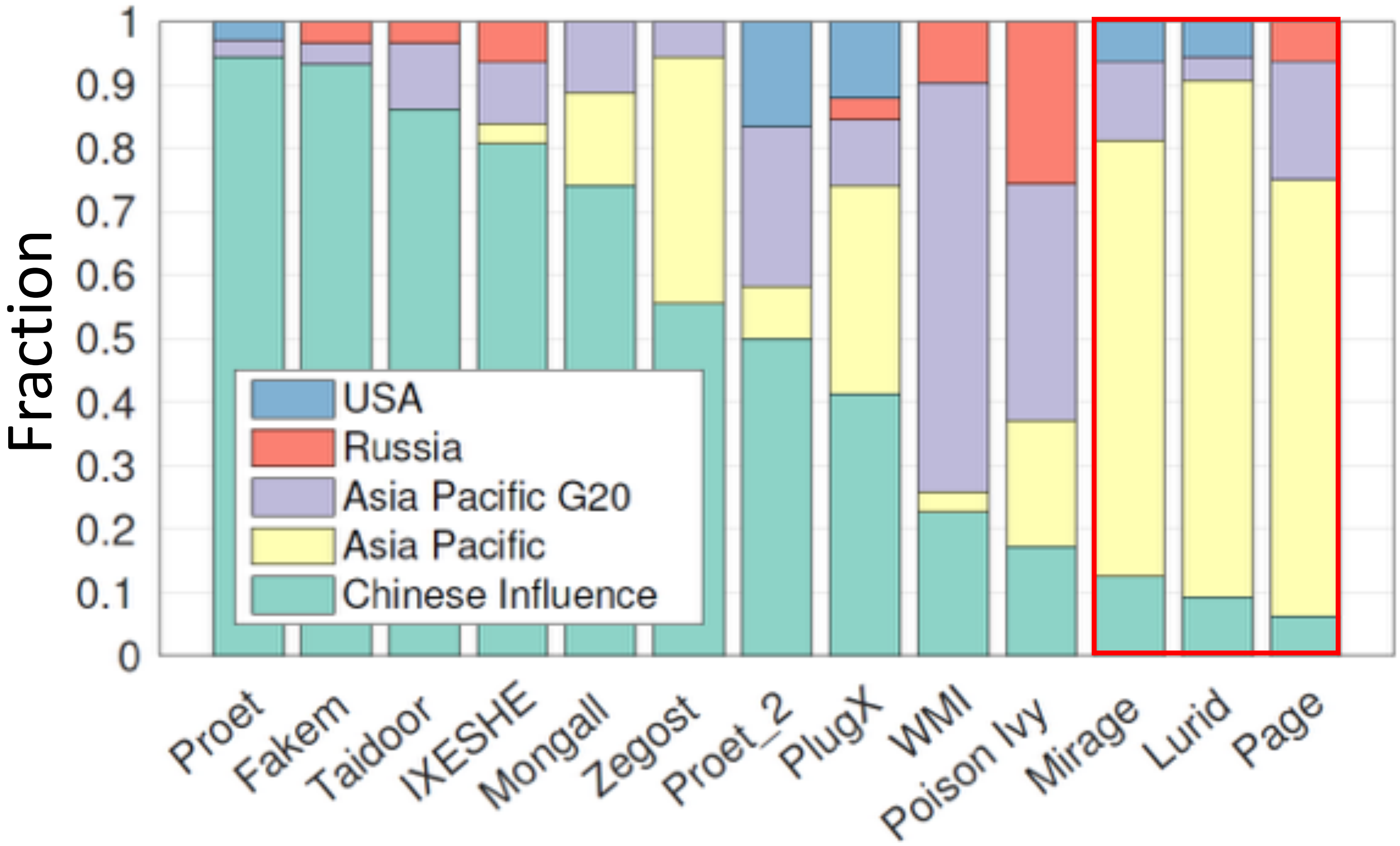
How do attacks faced by different groups compare with each other? Malware targeting (cont.)



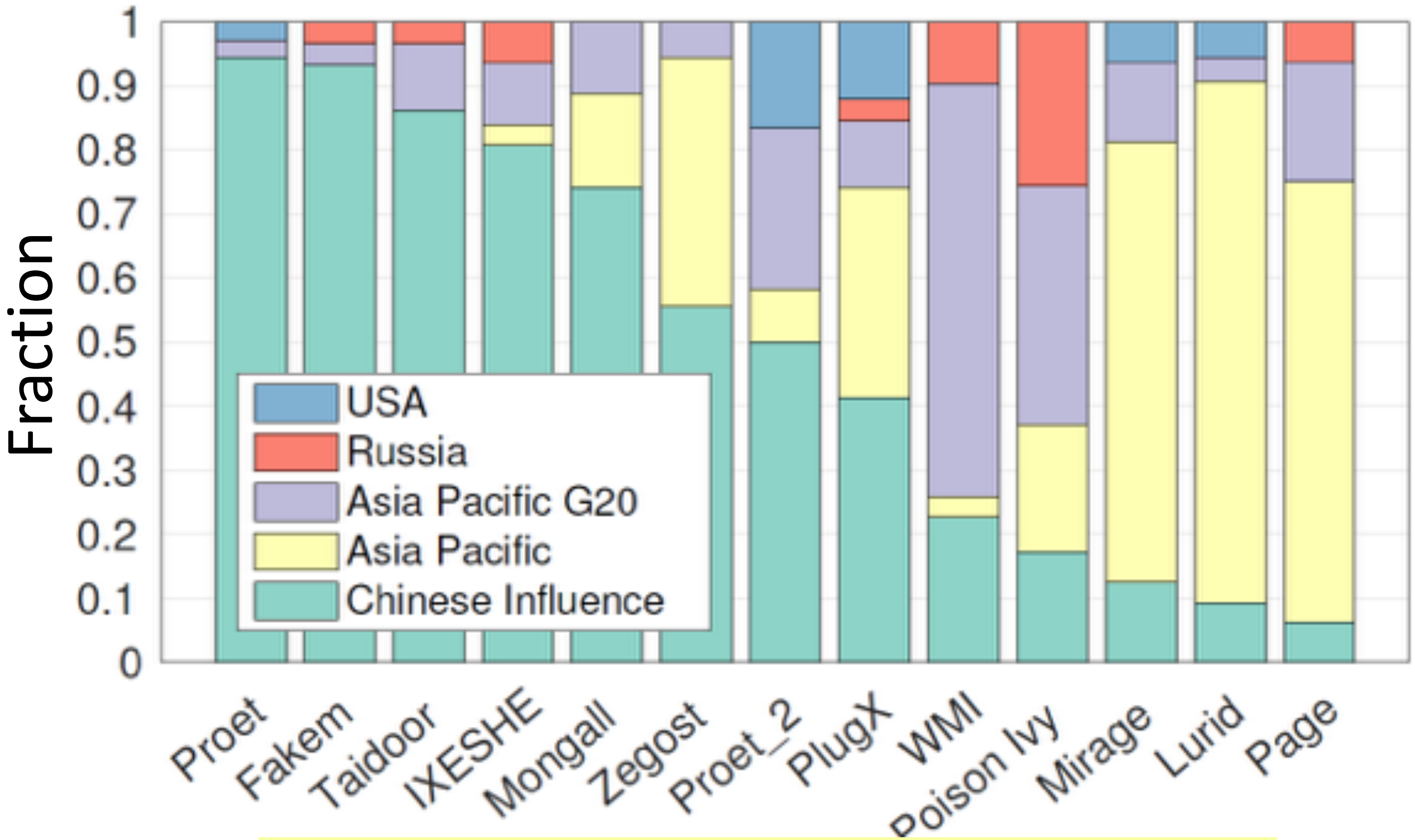
How do attacks faced by different groups compare with each other? Malware targeting (cont.)



How do attacks faced by different groups compare with each other? Malware targeting (cont.)



How do attacks faced by different groups compare with each other? Malware targeting (cont.)



Malware found in multiple countries tend to target a confined region

Outline

1) Methodology

2) Analysis of exploit documents

3) Future work

Future work

- Monitoring operator behavior of targeted malware
- Analysis of evasions techniques, attackers operations, and other attack vectors
- Deploy on-premises and cloud-based services for analysis of email attachments

Take home messages

- Complementary methodology to measure targeted attacks at scale
- At-risk groups upload exploit documents to VirusTotal
- Groups tend to be targeted with tailored decoys and malware families
- Preliminary impact
  - Service deployed at email provider with 100,000+ users
  - Dataset and academic service available at https://slingshot.dedis.ch

Frequently Asked Questions

- What are the observational biases of using VirusTotal?
- What are the common types of malicious documents that you filtered out?
- Why did you focus on exploit documents?
- What precautions did you take to reduce false negatives?
- Did you find indications of successful compromises?

stevens.leblond@epfl.ch

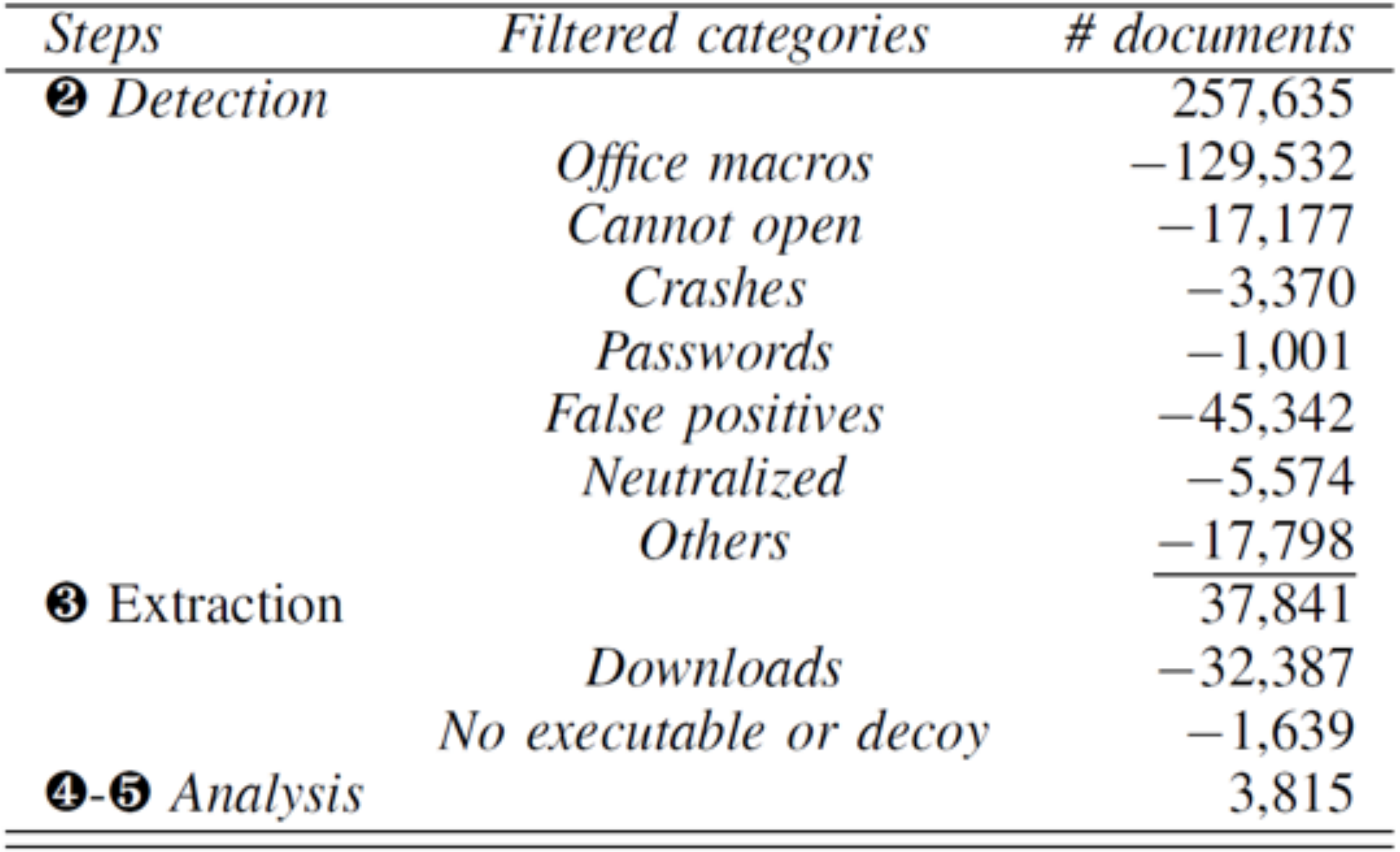
What are the observational biases of using VirusTotal?

- Coverage of targeted attacks is limited to those users and organizations who upload suspicious files

- VirusTotal’s visibility is likely skewed towards users who work with non-classified material

- VirusTotal dataset offers a partial coverage of attacks where individuals and NGOs are likely over-represented

What are the most common malicious documents that you filtered out?



Steps	*Filtered categories*	*# documents*
❷ *Detection*		257,635
	Office macros	−129,532
	Cannot open	−17,177
	Crashes	−3,370
	Passwords	−1,001
	False positives	−45,342
	Neutralized	−5,574
	Others	−17,798
❸ Extraction		37,841
	Downloads	−32,387
	No executable or decoy	−1,639
❹-❺ *Analysis*		3,815

Why did you focus on exploit documents?

- Exploit documents are the most common vector of targeted attacks identified by related work

- Macros require additional user approval and can be forcibly disabled by system administrators

- Used against a range of targets including NGOs, news agencies, and military, governmental and intelligence agencies

What precautions did you take to reduce false negatives?

- Reducing detection FNs
  - Cross validated EMET detection results with ground truth from the WUC dataset
  - 29/143 WUC documents were not detected by EMET, none of them FNs (16 Mac OS X, 9 wrong reader version, 2 password, and 2 without exploit)
- Reducing extraction FNs
  - Manually inspected EMET detections that didn’t write files to disk
  - 29/4,259 documents detected by EMET did not write any files to disk, none of them FNs (6 crashes, 4 experimental, and 19 dysfunctional)
- None of our analyses depends on the lack of evasion techniques in the malware embedded in exploit documents

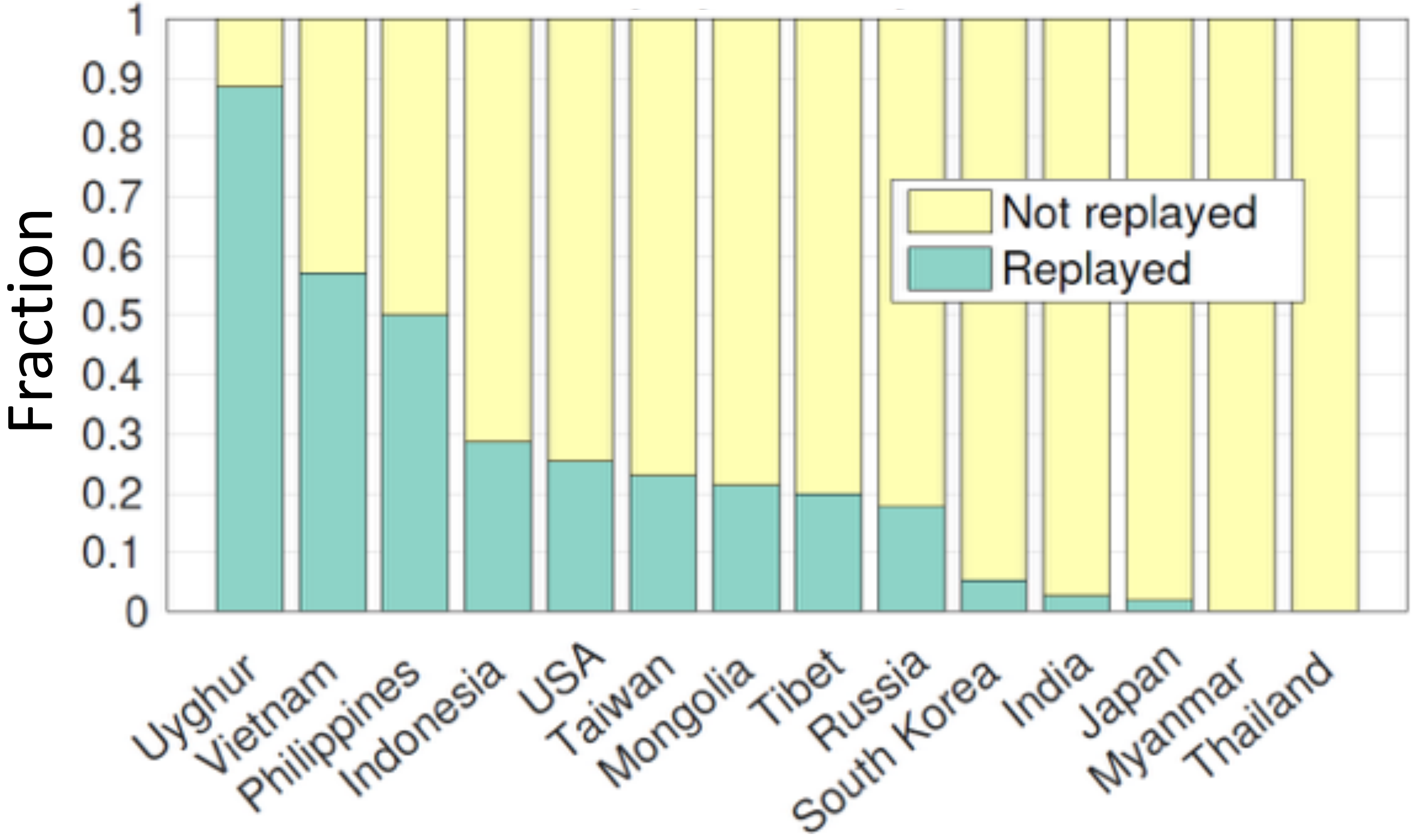
Did you find indication of successful compromises?

- Coded decoys based on their languages, the countries they refer to, ethnic groups and dates, and whether they targeted specific individuals or organizations

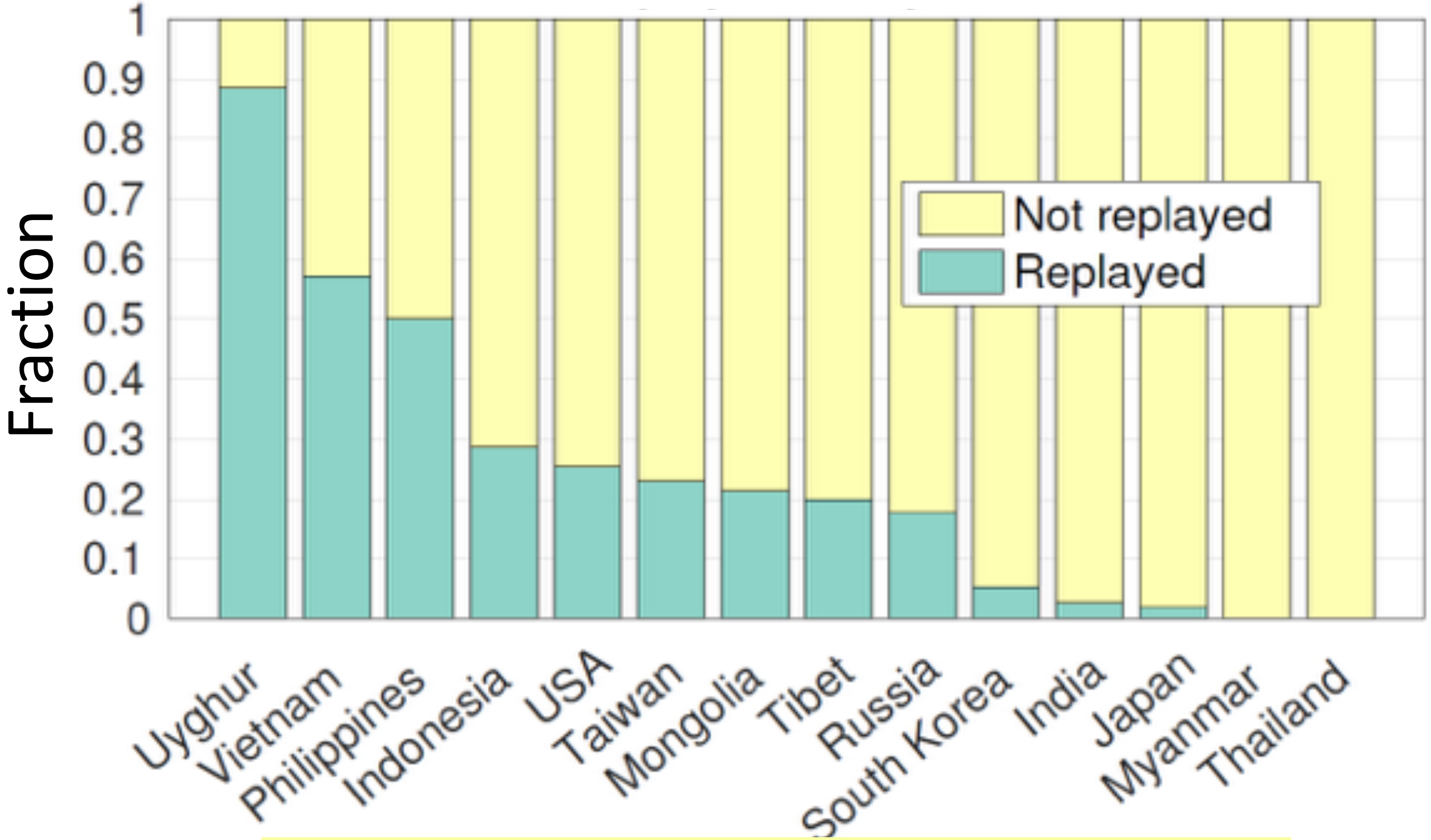
- Native speakers independently coded the documents written in Russian, Traditional Chinese, Uyghur, and Vietnamese

- Identified documents likely exfiltrated from compromised systems and used as decoys in exploit documents targeting new, related victims

Did you find indication of successful compromises (cont.)?



Did you find indication of successful compromises (cont.)?



Most groups were targeted with replayed decoys

Did you find evidence of zero-day vulnerabilities?

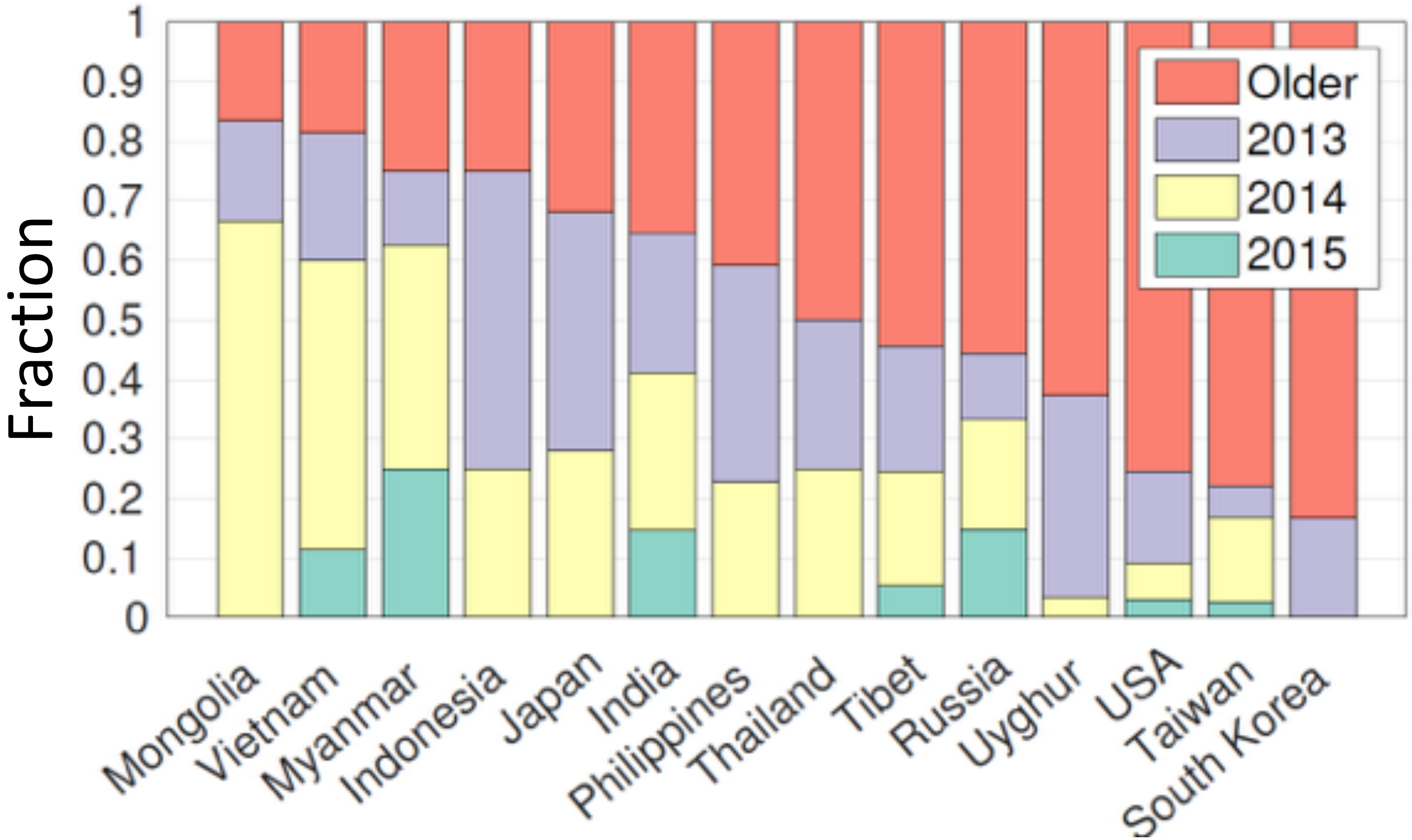
- We collaborated with a large AV vendor to determine the CVE tags of the exploited reader vulnerabilities
- The vendor scanned all the exploit documents that we detected and compared the resulting CVE with the majority of VirusTotal tags
  - If the two CVEs matched, no further action was taken
  - Otherwise, the sample was analyzed manually
- Samples for which the CVE release date was after the date of upload on VirusTotal were examined manually to determine the CVE’s correctness
- Based on this methodology, we didn’t find evidence of zero-day vulnerabilities

Can you estimate the dates of the decoys?

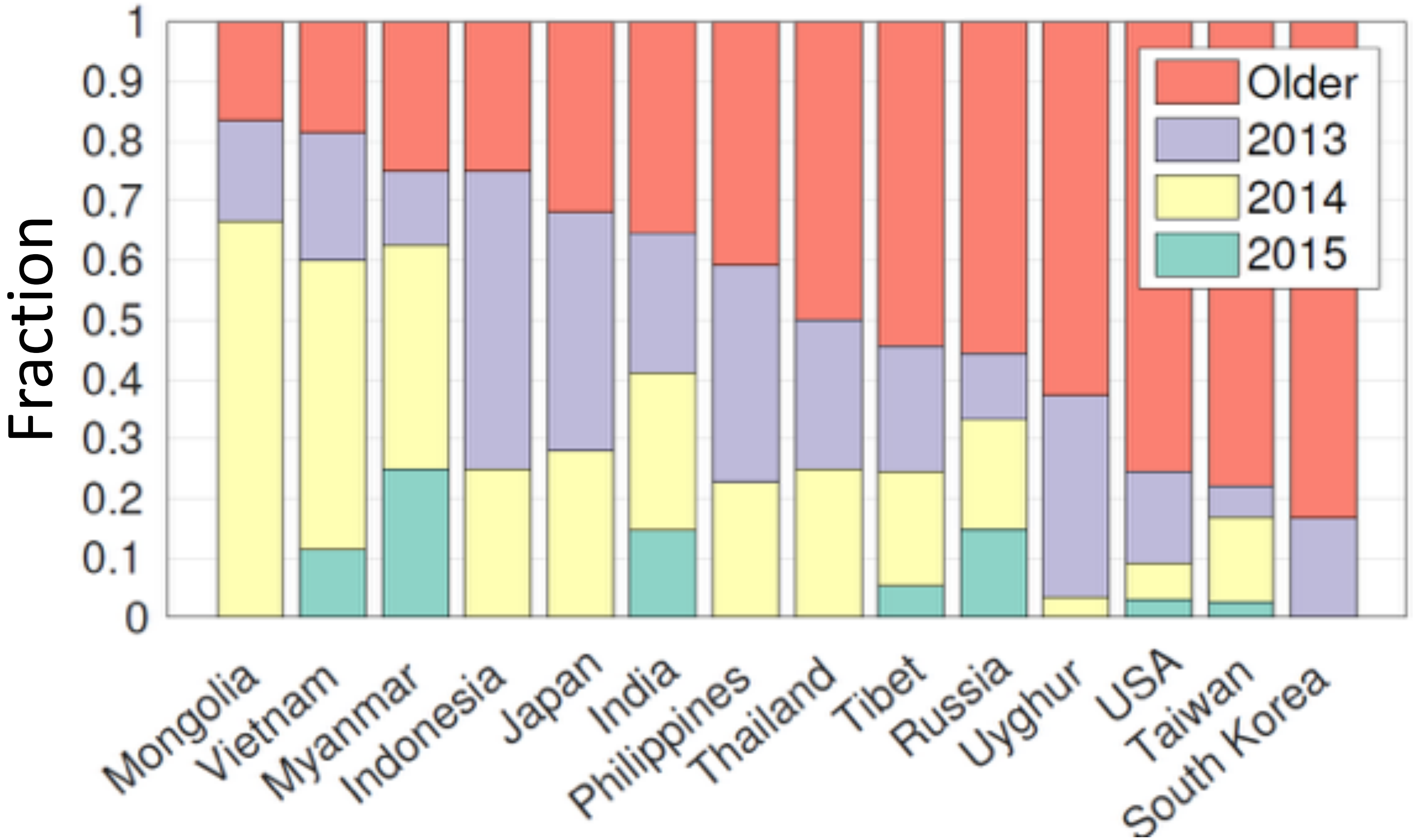
- We coded decoys according to their languages, the countries they refer to, ethnic groups and dates, and whether they targeted specific individuals or organizations

- Native speakers independently coded the documents written in Russian, Traditional Chinese, Uyghur, and Vietnamese

Can you estimate the dates of the decoys (cont.)?



Can you estimate the dates of the decoys (cont.)?



All groups exhibited decoys referring to a least one year in 2013-2015