Security Information Quality Provided by News Sites and Twitter

Ryu SAEKI, Kazumasa OIDA
mfm22105@bene.fit.ac.jp

Fukuoka Institute of Technology, Fukuoka, Japan

Resume

Mar 2022: Graduated from university

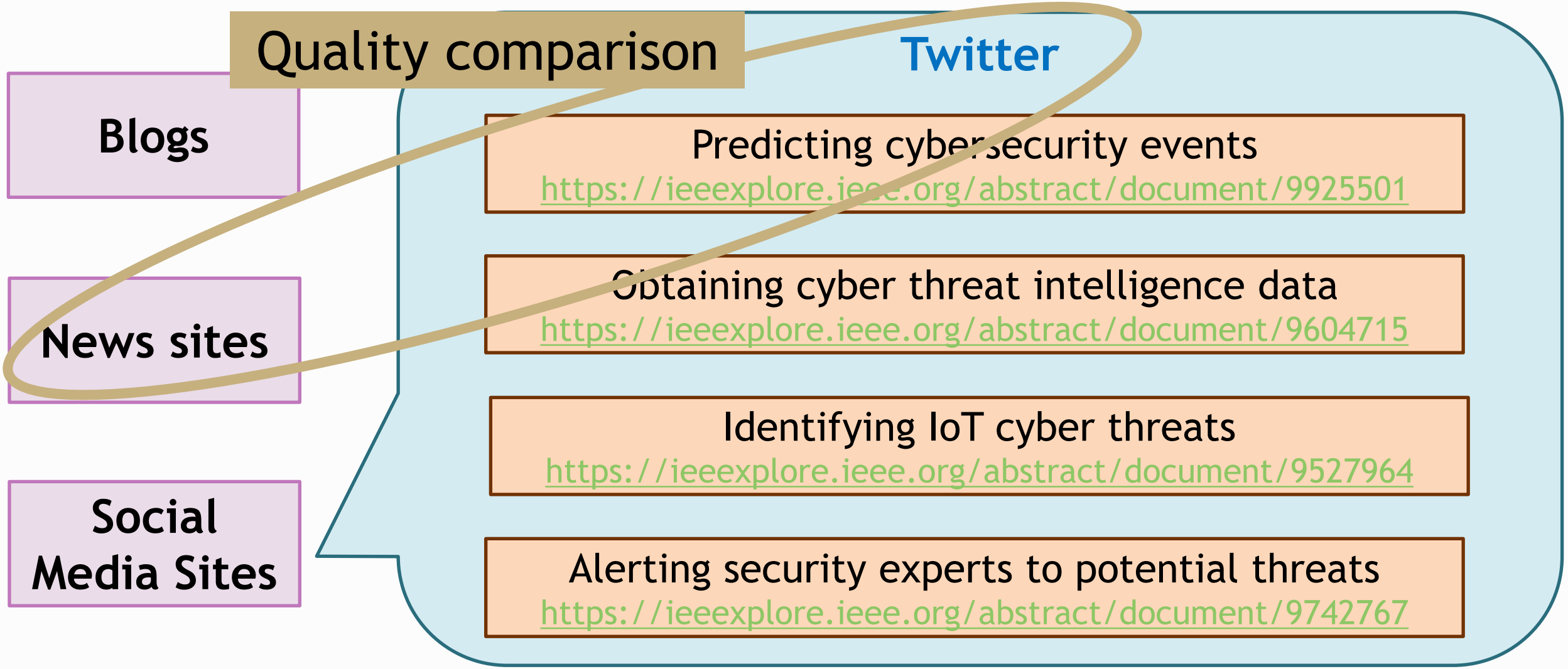
- Major: Computer Science and Engineering

Apr 2022: Entered graduate school

- Major: Computer Science and Engineering
- First year of Master's program

Future: Become an engineer in the field of cybersecurity

Background and Motivation



Case Study

Topic: Emotet

Target: Japan

Period: 2019/1/1 - 2022/10/31

Quality comparison

News site

Security NEXT

Case Study

Topic

Emotet

Target

Japan

Period

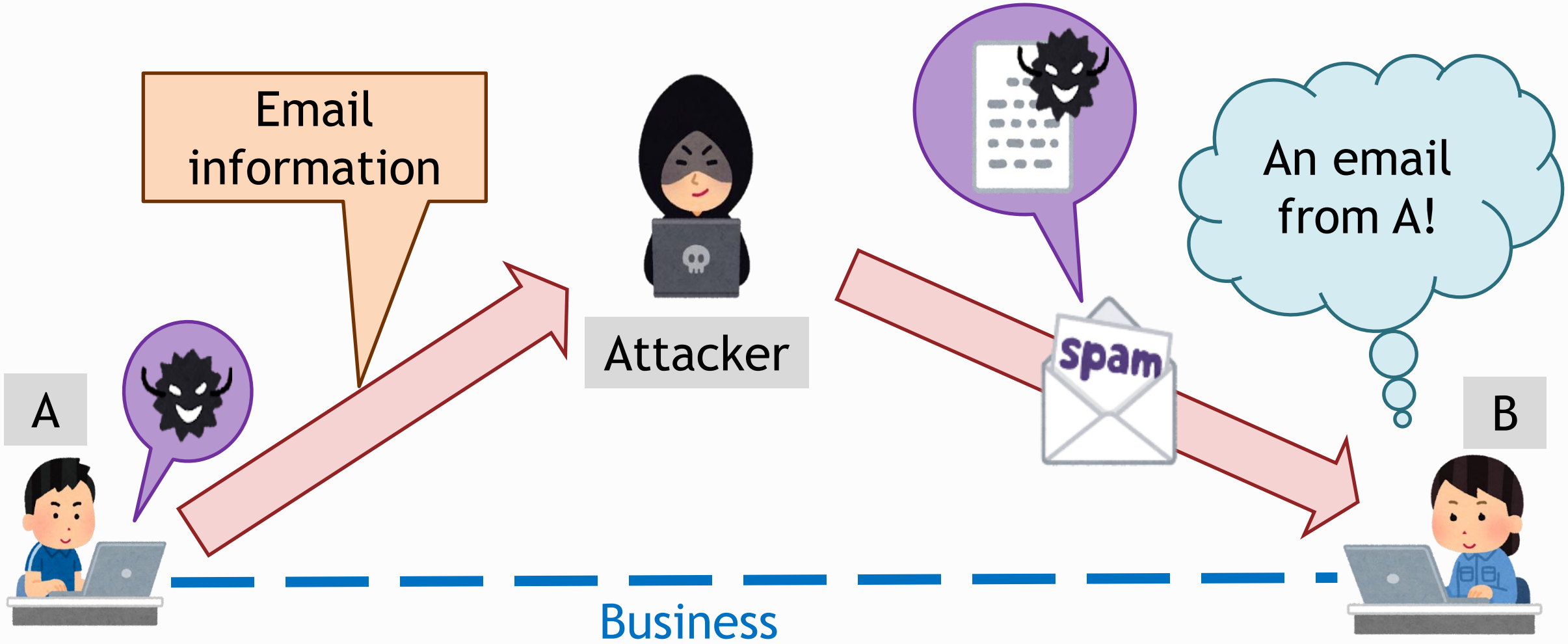
2019/1/1 - 2022/10/31

Quality comparison

News site

Security NEXT

Emotet


Email information
Attacker
An email from A!
A
B
Spam
Business

Case Study

Topic

Emotet

Target

Japan

Period

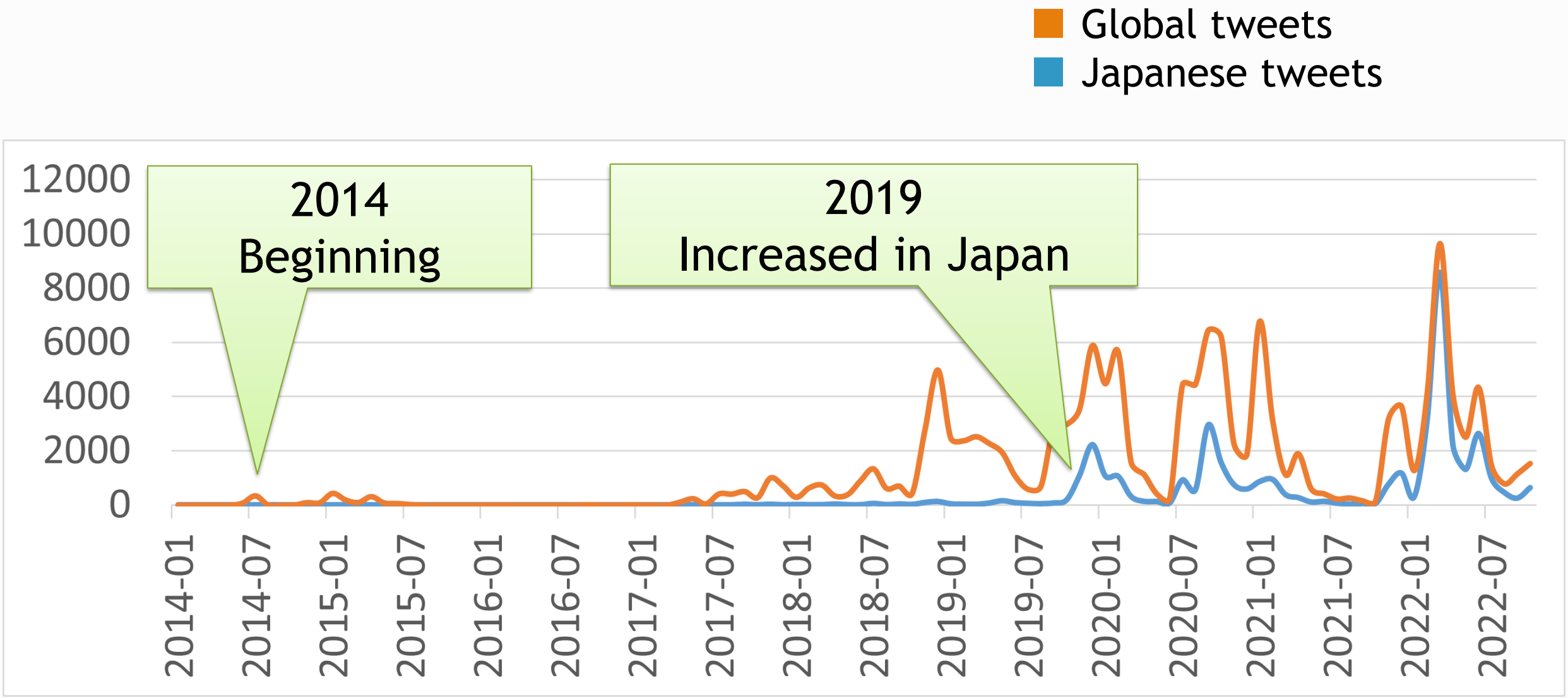
2019/1/1 - 2022/10/31

Quality comparison

News site

Security NEXT

Emotet Tweets



Case Study

Topic

Emotet

Target

Japan

Period

2019/1/1 - 2022/10/31

Quality comparison

News site

Security NEXT

Security NEXT

Operating company

NEWSGAIA Co., Ltd.

Free access

Topic

Information Security

First published

2004

Large number of articles

Case Study

Topic

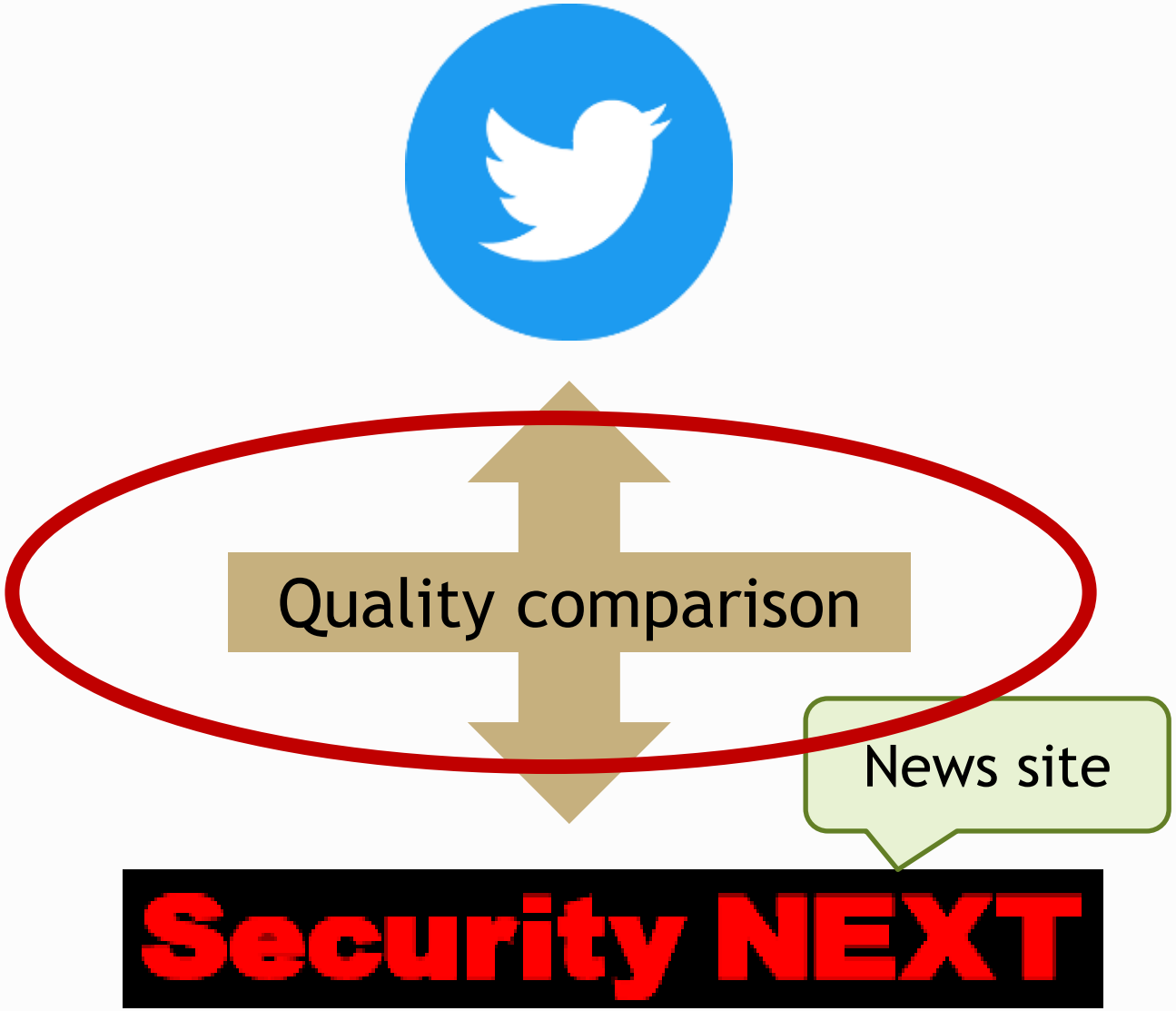
Emotet

Target

Japan

Period

2019/1/1 - 2022/10/31



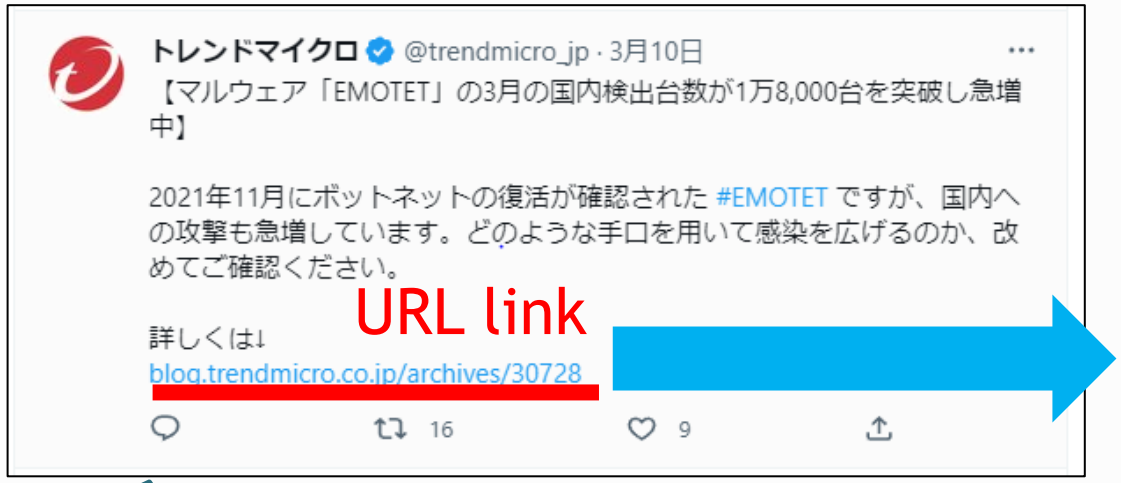
Comparison Method

■ Level of detail

■ Real-time performance

■ Reliability

Data Collection from Twitter



URL link

Tweet

Linked website

Word (noun)

2021年1月に一旦テイクダウンされたものの、2021年11月から活動を再開したマルウェア「EMOTET」が、その後、日本国内でも被害が拡大する状況となっています。

Data Collection from Security NEXT

Security NEXT article

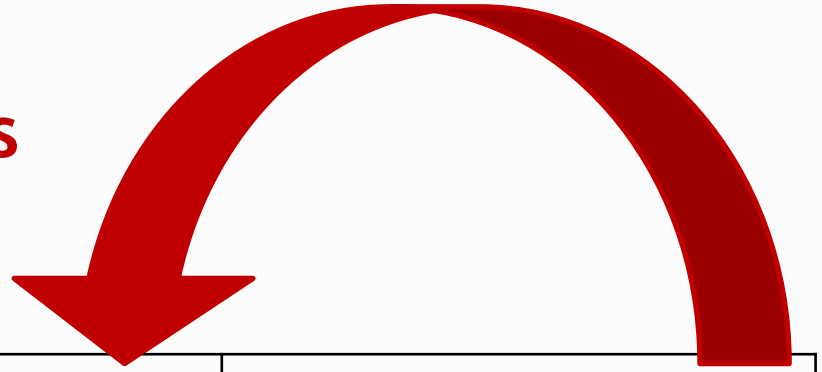
"Emotet" in the title

クラシエホールディングスは、マルウェア「Emotet」の感染により、従業員を装った「なりすましメール」が出回っていることを明らかにした。

Word(noun)

Dataset Size

18 times



	Twitter	Security NEXT
# websites	1,660	91
# words collected	262,584	6,100
# unique words collected	42,347	2,091

Elements of Comparison

◆ Malicious file extension

- ZIP
- DOC
- PDF
- LNK
- XLS
- RTF

◆ Spam email subject line

- COVID-19
- Invoice
- Bonus
- Conference
- Questionnaire
- Fire Inspection

◆ Malware distributed by Emotet

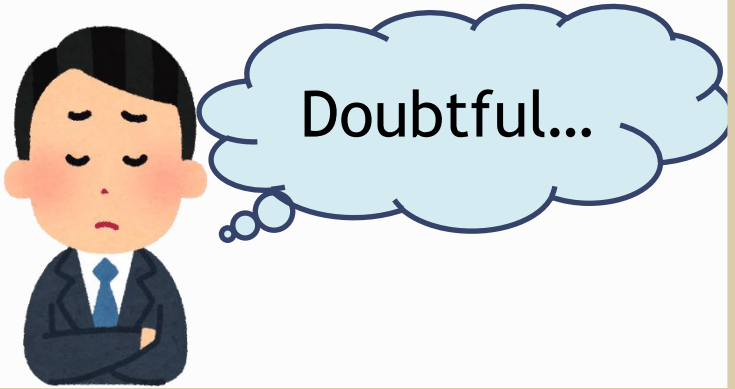
- TrickBot
- IcedID
- Ryuk
- QakBot
- ZeusPandaBanker
- Gootkit
- Conti
- Cobalt Strike
- Ursnif
- Zloader

Comparison Method

■ Level of detail

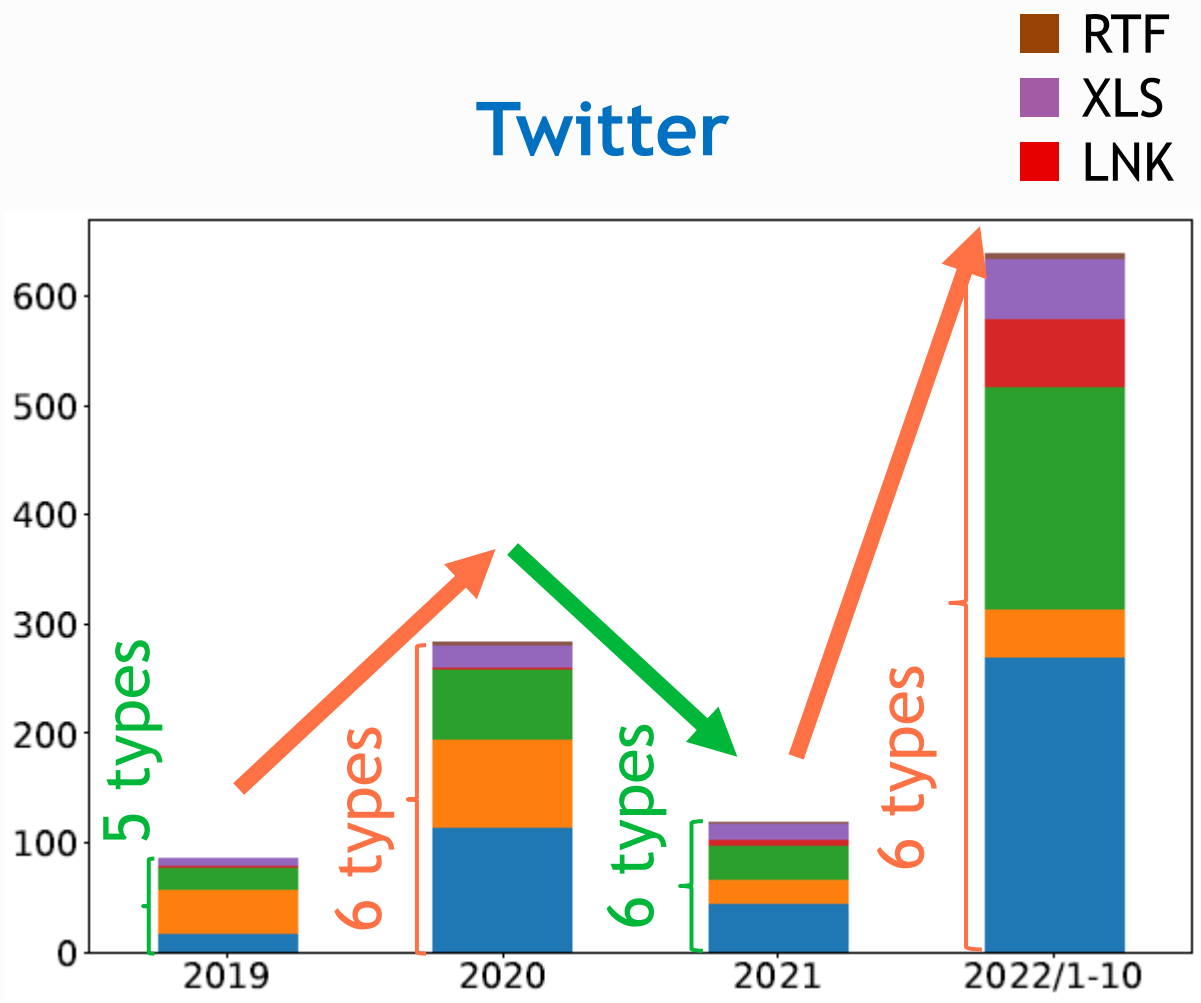
■ Real-time performance

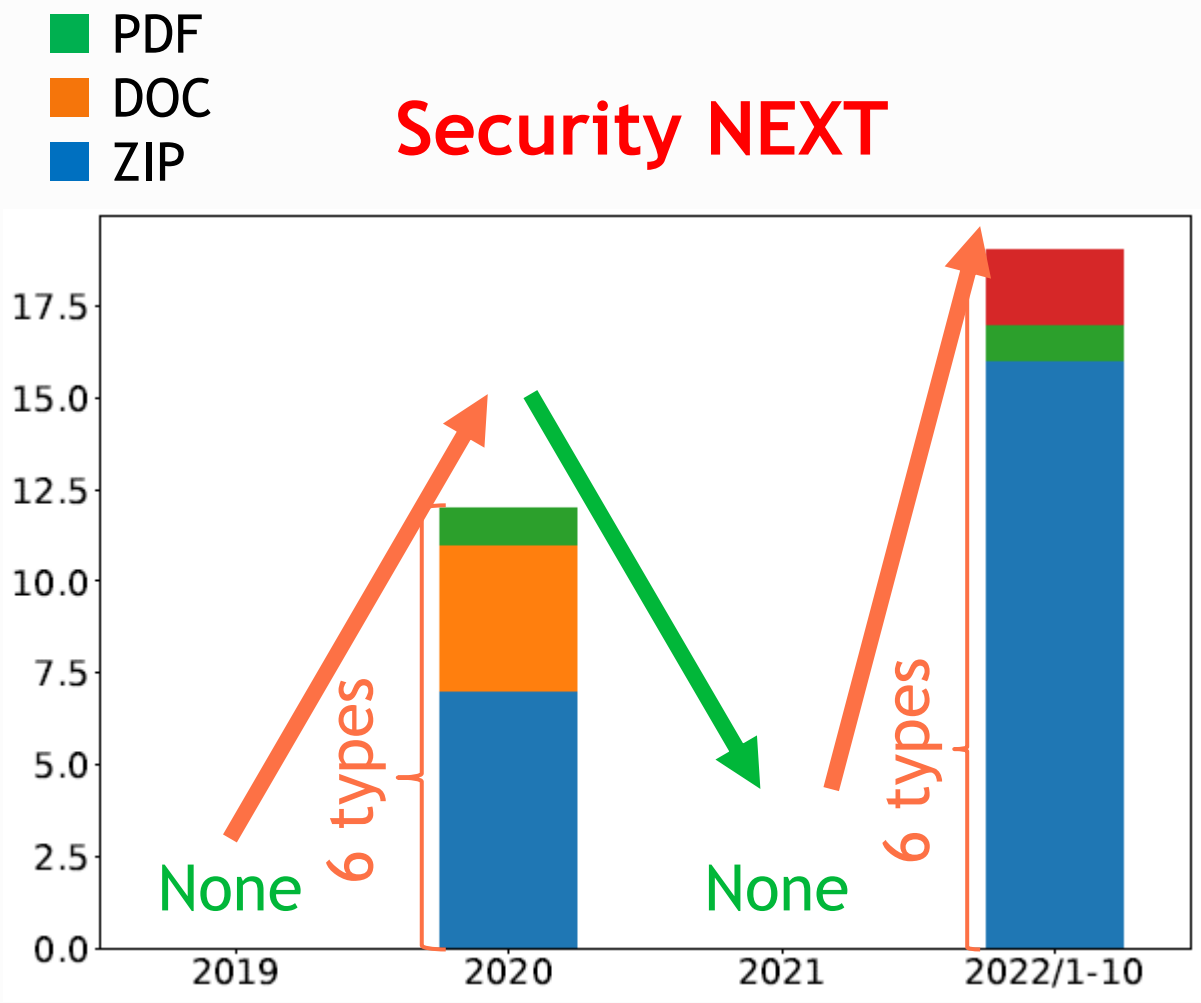
■ Reliability



Level of Detail

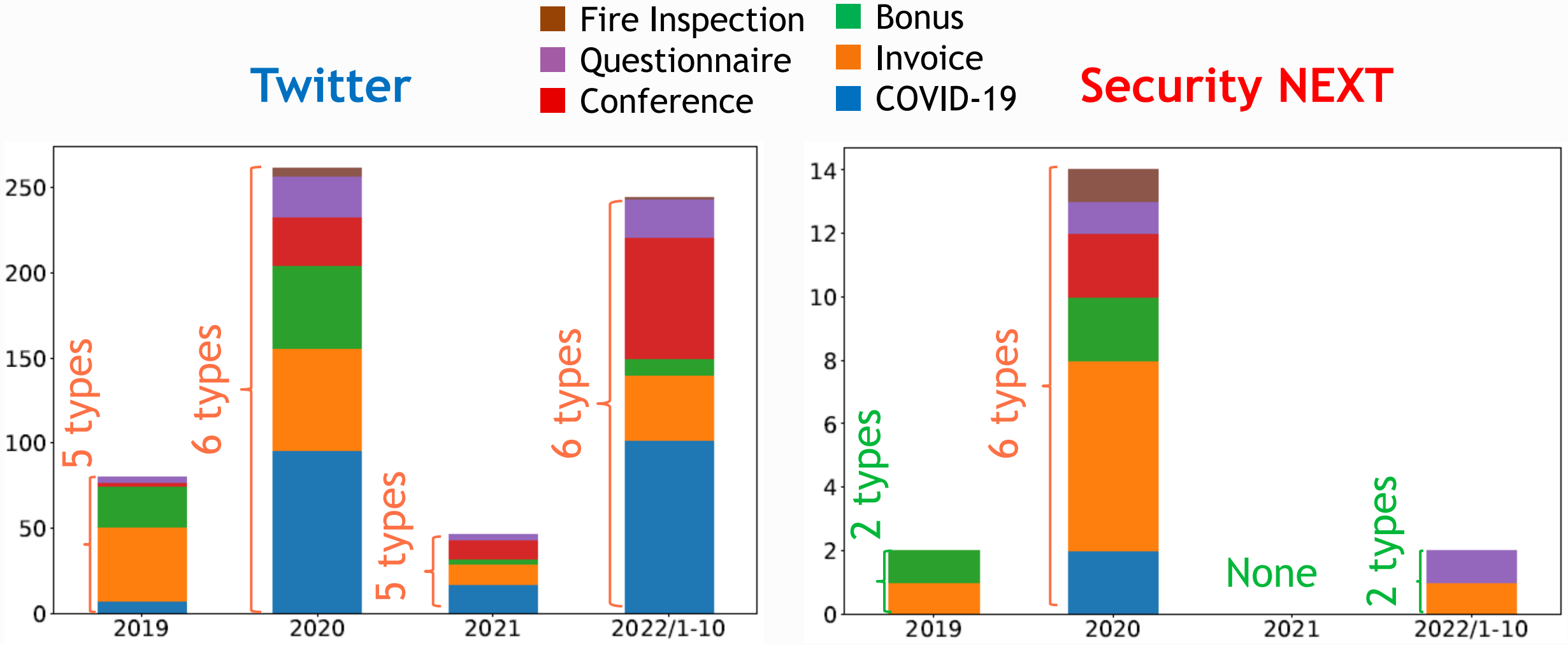
Malicious File Extension





Level of Detail

Spam Email Subject Line

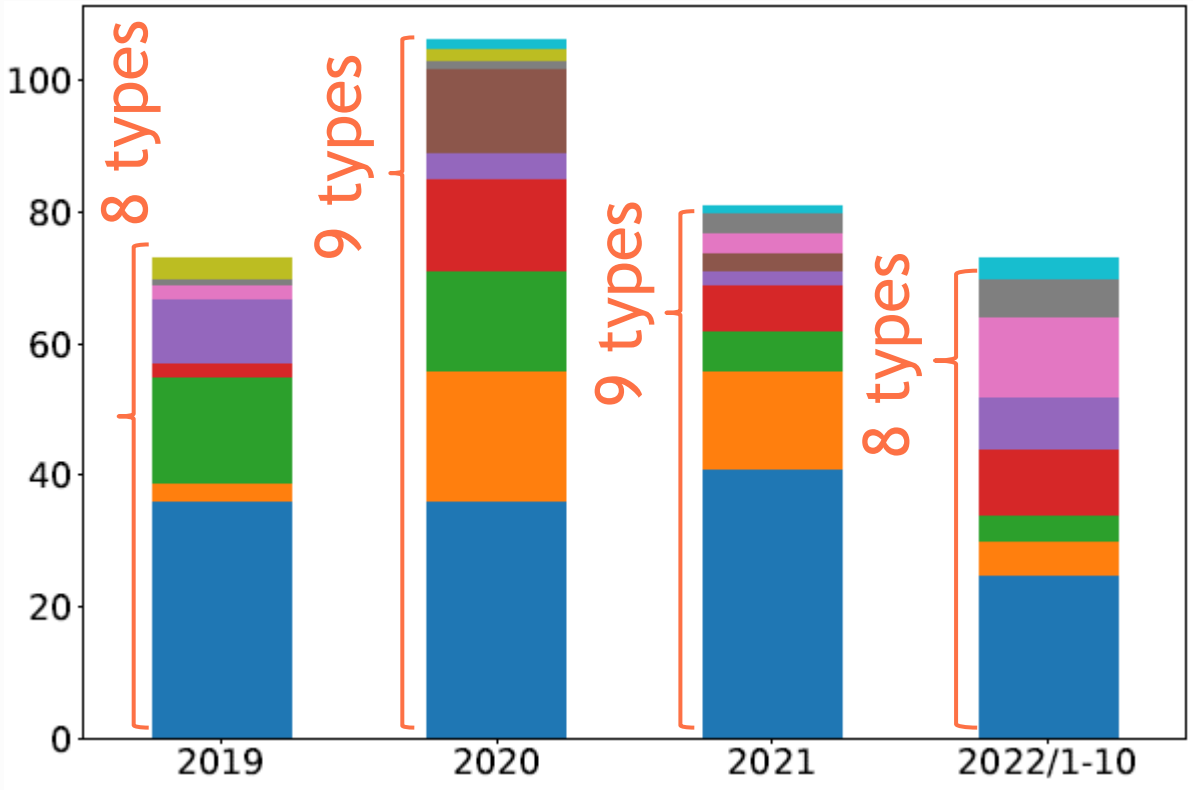


Level of Detail

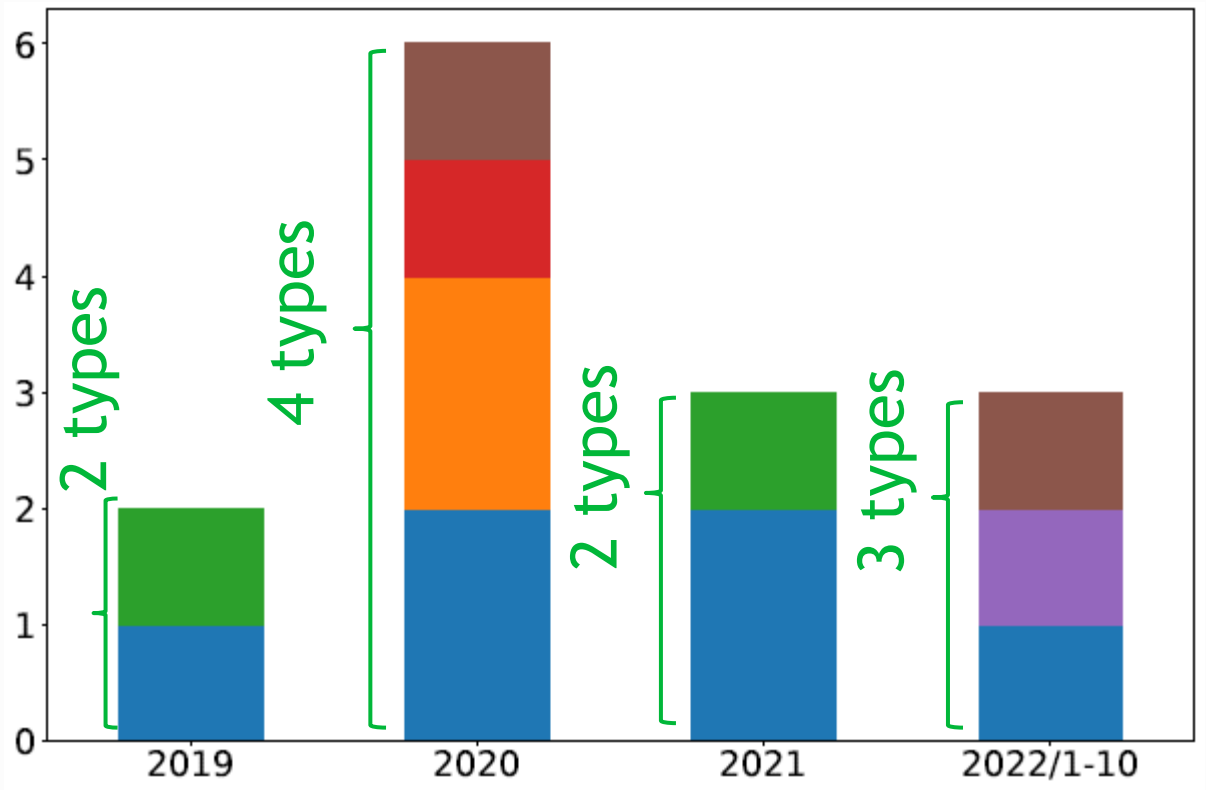
Malware Distributed by Emotet

Gootkit
ZeusPandaBanker
Cobalt Strike
Conti
Zloader
Ursnif
QakBot
Ryuk
IcedID
TrickBot

Twitter



Security NEXT

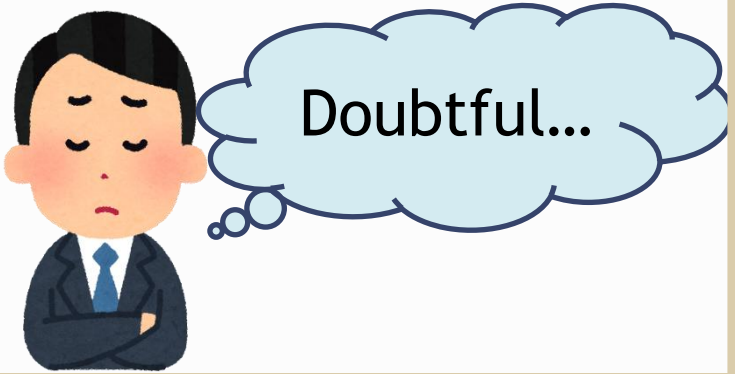


Comparison Method

■ Level of detail

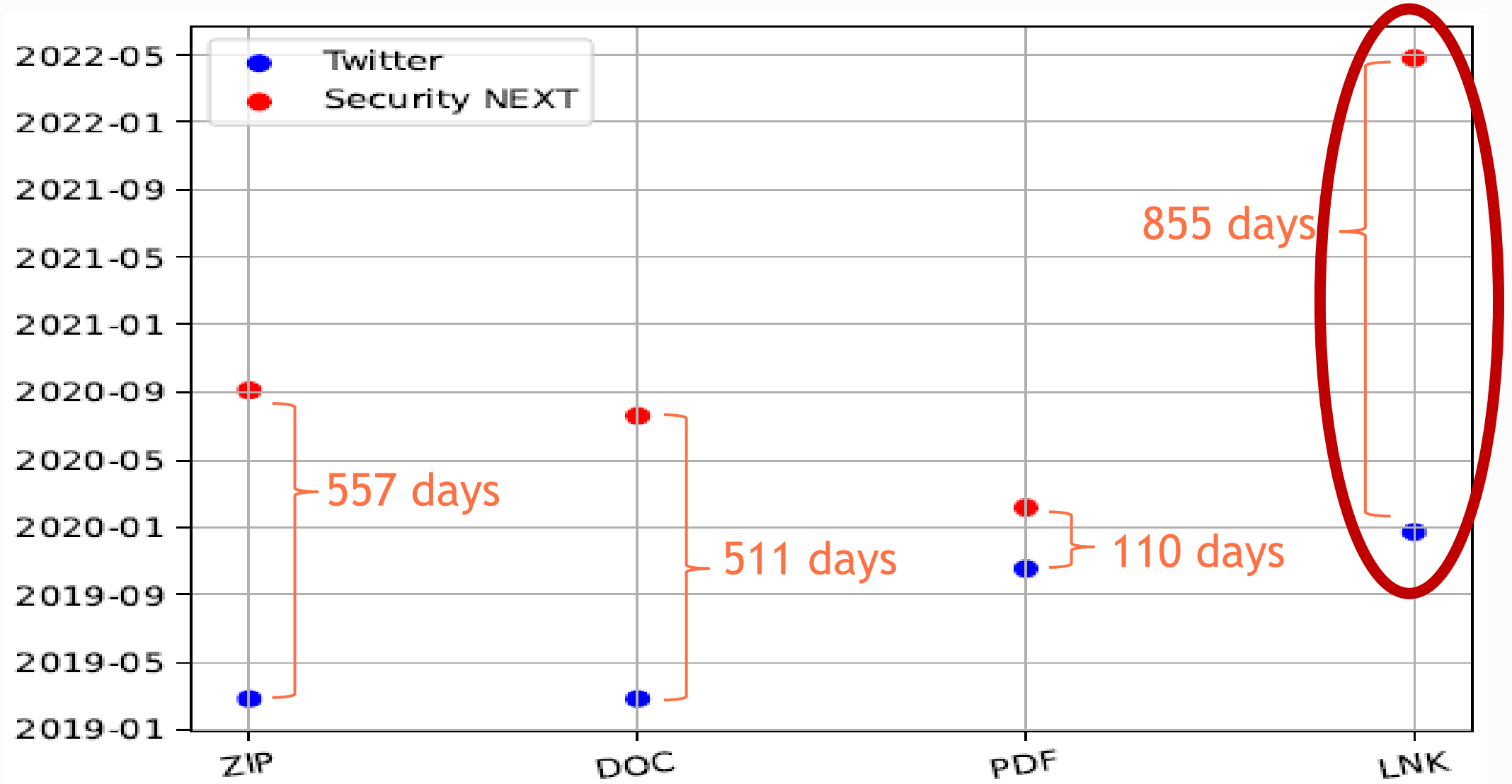
■ Real-time performance

■ Reliability



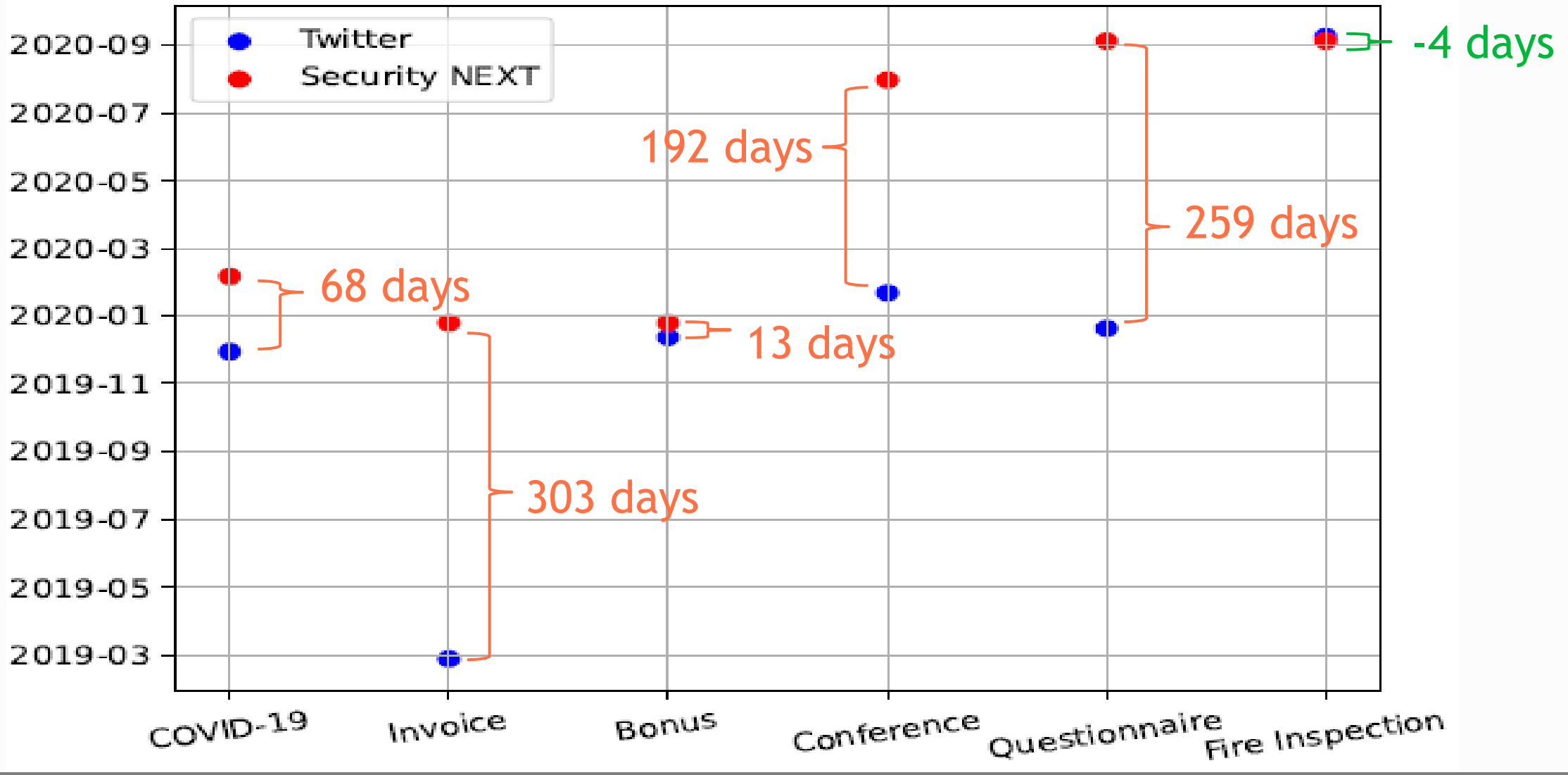
Real-time Performance

Malicious File Extension

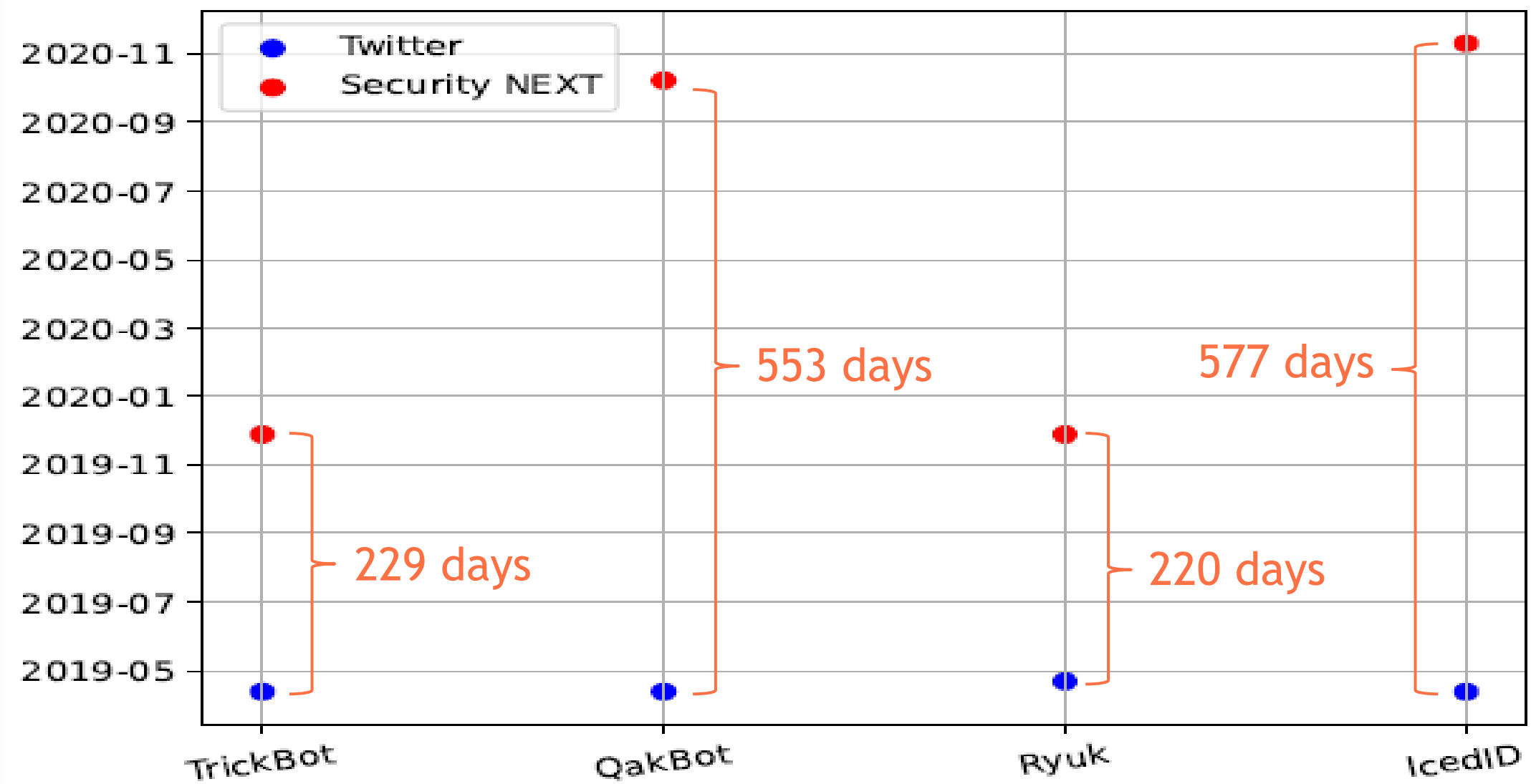


Real-time Performance

Spam Email Subject Line



Real-time Performance Malware Distributed by Emotet



Comparison Method

■ Level of detail

■ Real-time performance

■ Reliability

Reliability

	Factors of website reliability	Twitter	Security NEXT
1	The writer's name	20 / 20	20 / 20
2	The writer's contact information	13 / 20	20 / 20
3	Published or updated date	20 / 20	20 / 20
4	SSL certificate	20 / 20	20 / 20
5	Sources with links	14 / 20	1 / 20
6	No link errors	8 / 20	20 / 20
7	No misspellings	18 / 20	20 / 20
8	The privacy policy	13 / 20	20 / 20
	Total	**113 / 160**	**141 / 160**

Summary

■ Level of detail ■ Real-time performance ■ Reliability

Twitter	>>	Security NEXT
Malicious file extension		
5 ～ 6 types		0 ～ 6 types
Spam email subject line		
5 ～ 6 types		0 ～ 6 types
Malware distributed by Emotet		
8 ～ 9 types		2 ～ 4 types

Twitter	>>	Security NEXT
Malicious file extension		
Publish delay		110 ～ 855 days
Spam email subject line		
Publish delay		-4 ～ 303 days
Malware distributed by Emotet		
Publish delay		220 ～ 577 days

Twitter	≲	Security NEXT
Total score		
113 / 160		141 / 160
Sources with links		
14 / 20		1 / 20
No link errors		
8 / 20		20 / 20

Thank you for your attention!