

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

Quality comparison

Twitter

Blogs

Predicting cybersecurity events

<https://ieeexplore.ieee.org/abstract/document/9925501>

News sites

Obtaining cyber threat intelligence data

<https://ieeexplore.ieee.org/abstract/document/9604715>

Social
Media Sites

Identifying IoT cyber threats

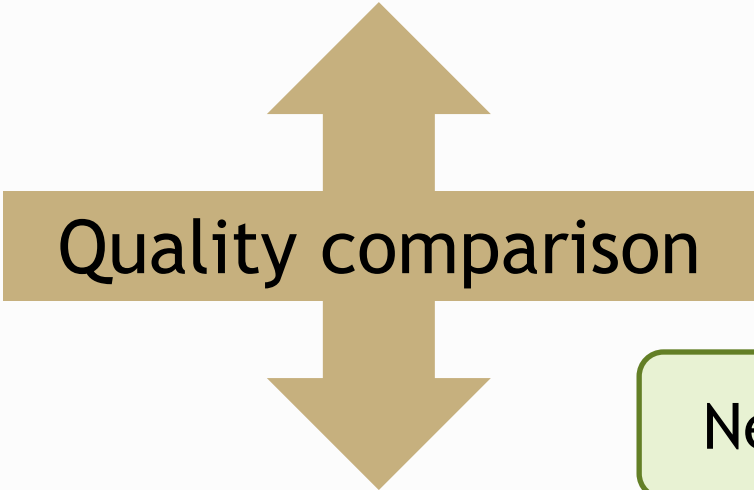
<https://ieeexplore.ieee.org/abstract/document/9527964>

Alerting security experts to potential threats

<https://ieeexplore.ieee.org/abstract/document/9742767>

Case Study

Topic	Emotet
Target	Japan
Period	2019/1/1 - 2022/10/31



News site

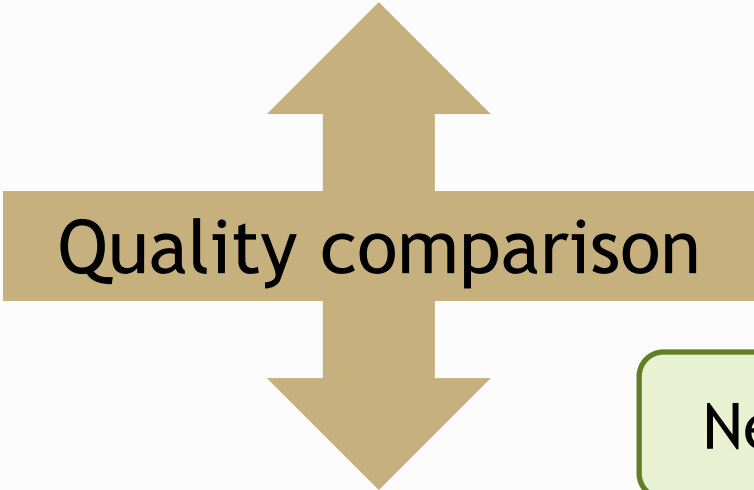
Security NEXT

Case Study

Topic
Emotet

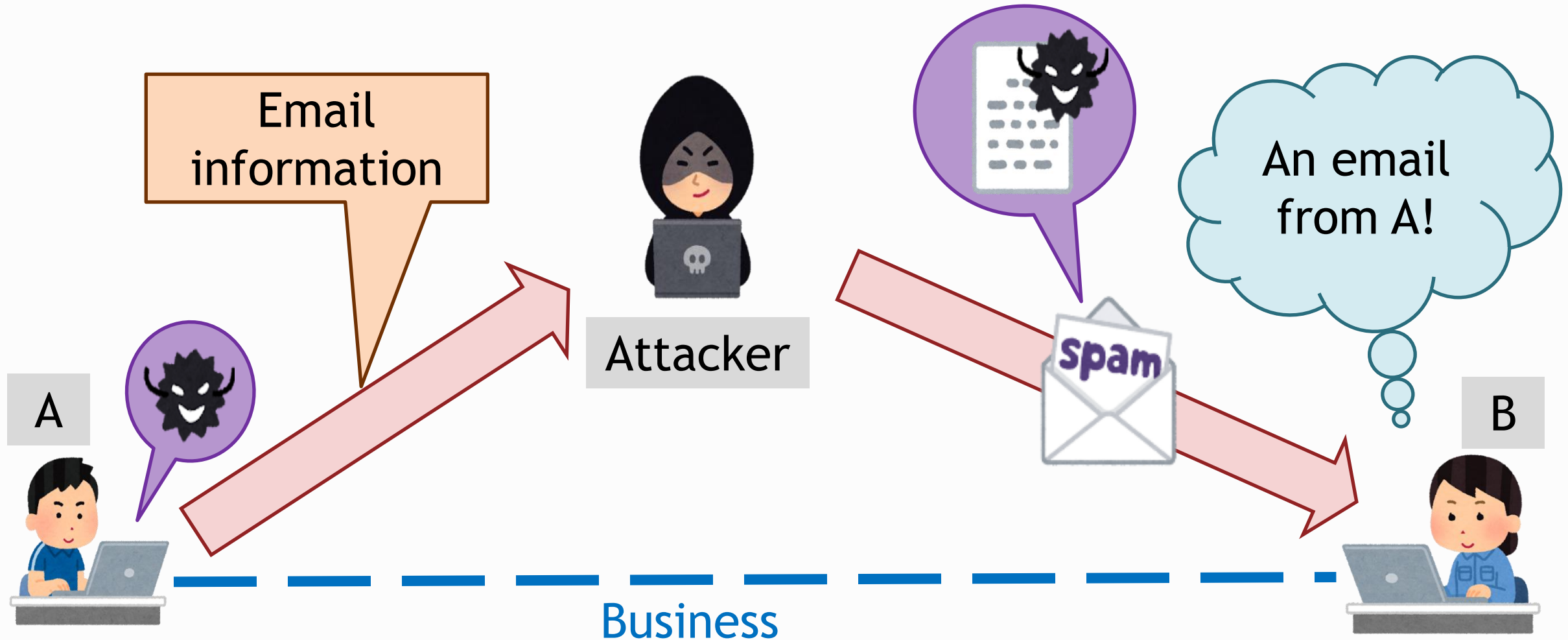
Target
Japan

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



Security NEXT

Emotet

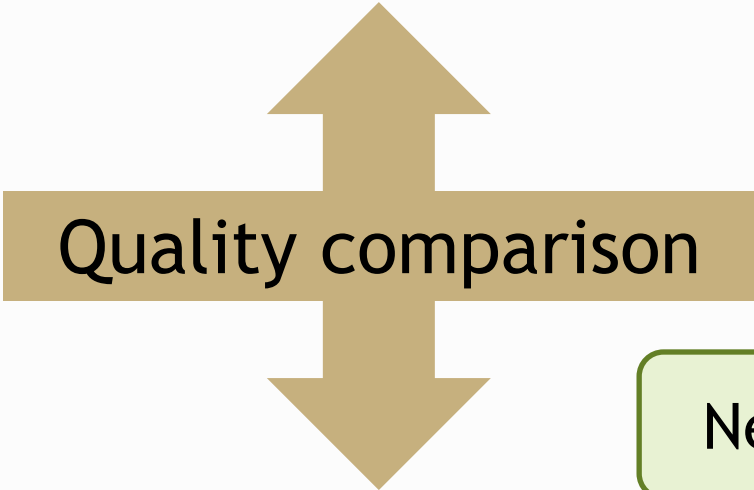


Case Study

Topic
Emotet

Target
Japan

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

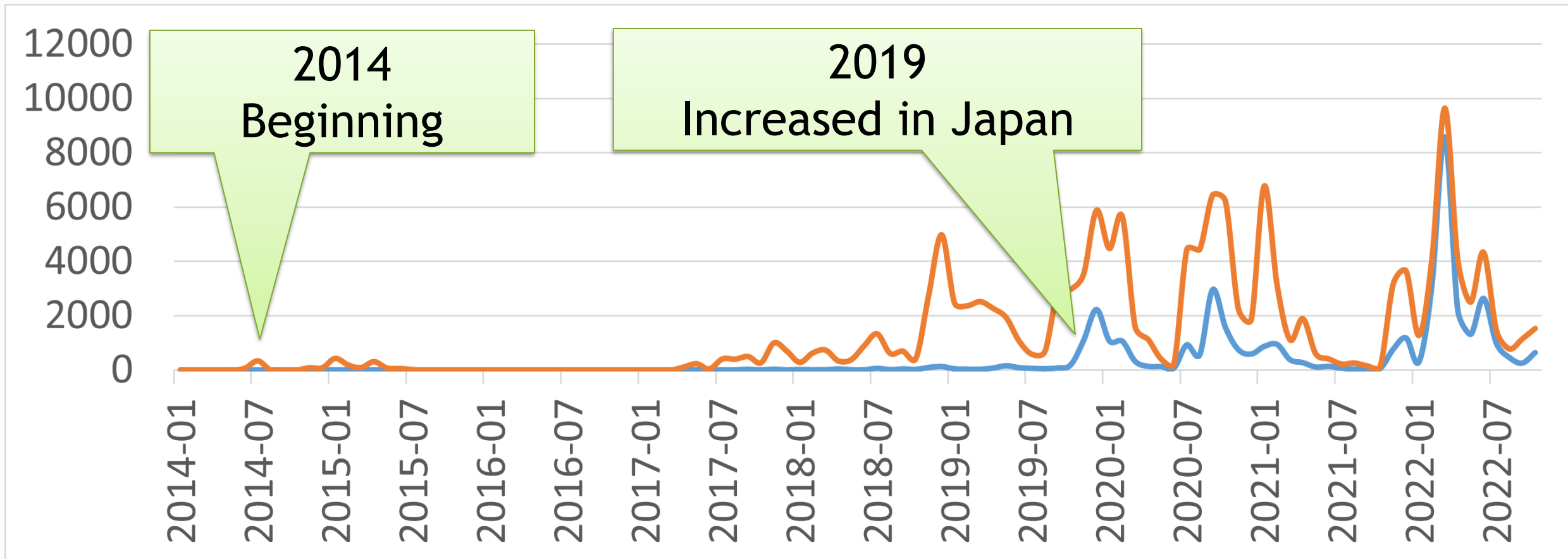


News site

Security NEXT

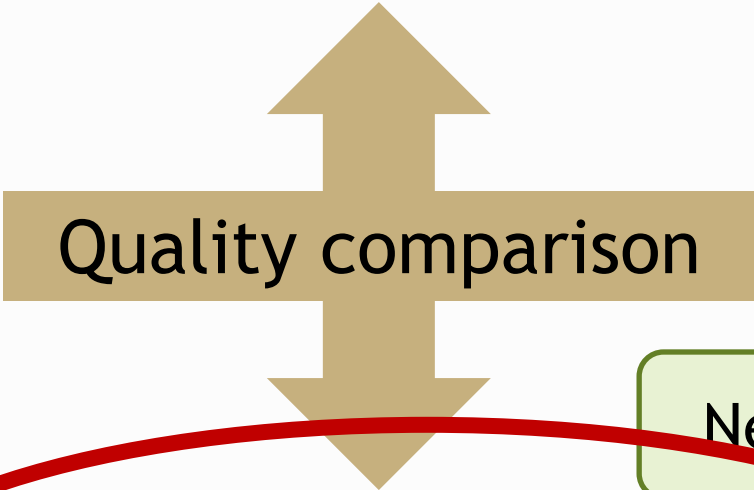
Emotet Tweets

- Global tweets
- Japanese tweets



Case Study

Topic	Emotet
Target	Japan
Period	2019/1/1 - 2022/10/31



News site



Security NEXT

Operating company
NEWSGAIA Co., Ltd.

Topic
Information Security

First published
2004

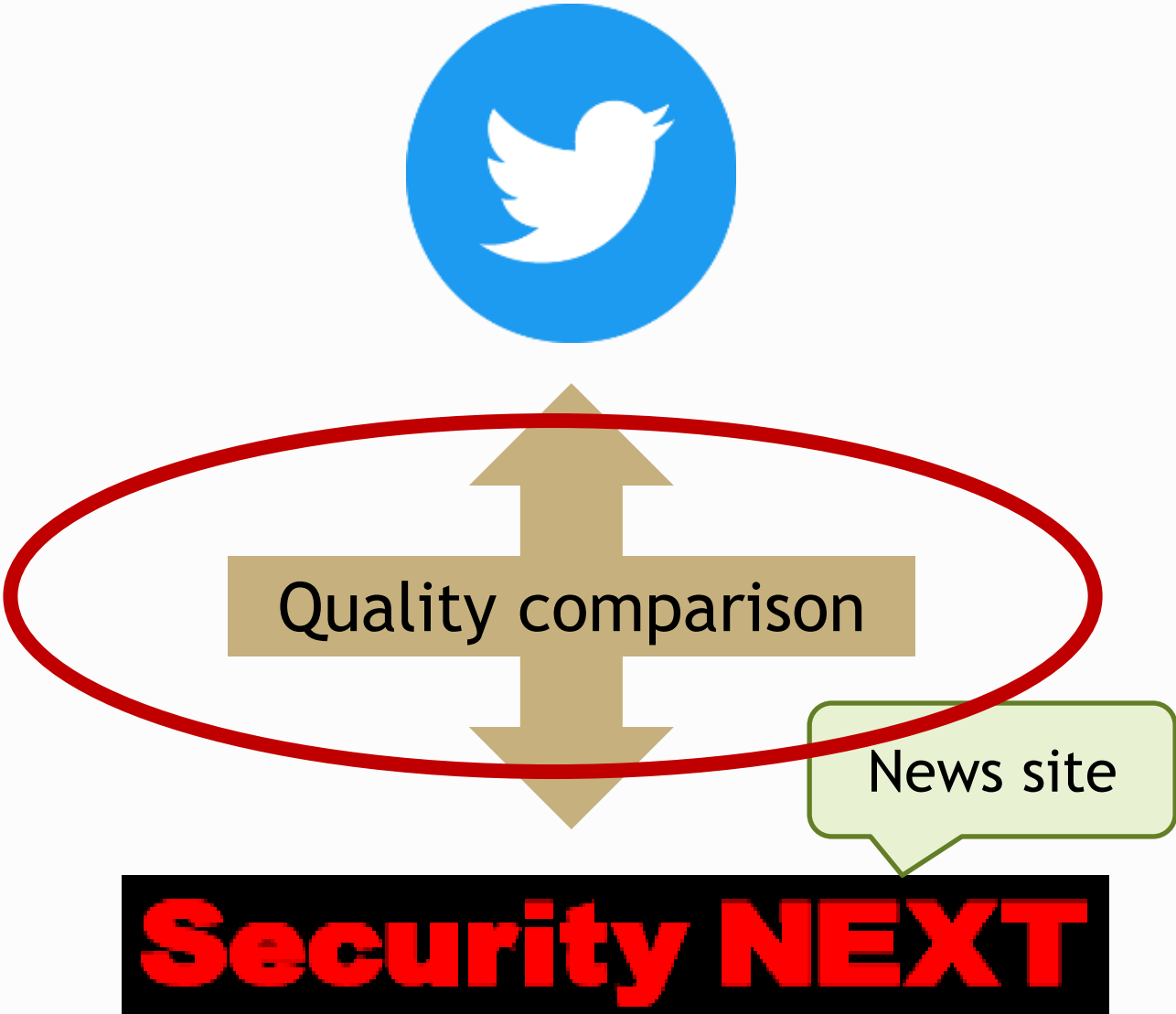
Free access

Large number of
articles

The screenshot shows the Security NEXT website interface. At the top, there's a navigation bar with categories like 'ニュース' (News), '政府・業界動向' (Government/Industry Trends), '脆弱性' (Vulnerabilities), '製品・サービス' (Products/Services), 'コラム' (Columns), '過去記事' (Past Articles), and 'メルマガ' (Newsletter). A search bar is on the right. Below the navigation, there's a promotional banner for 'Astera for business' with a price of ¥3,480/month. The main content area features a list of news articles with dates and titles, such as '大阪急性期・総合医療センターにサイバー攻撃 - 電子カルテが被害' (2022/11/01) and 'メール転送エージェント「Exim」のDMARC関連処理に脆弱性' (2022/11/01). On the right side, there are several advertisements, including one for 'EdgeTech+' and another for 'Adaptive' TOEIC preparation courses. A 'ピックアップ' (Pickup) section at the bottom right highlights recent security news.

Case Study

Topic	Emotet
Target	Japan
Period	2019/1/1 - 2022/10/31

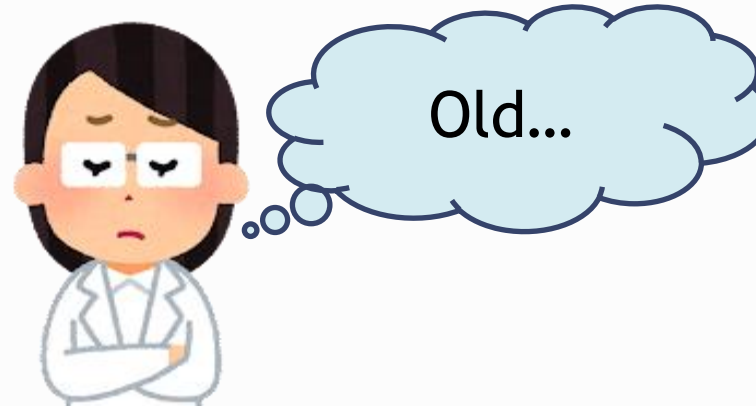


Comparison Method

■ Level of detail



■ Real-time performance



■ Reliability



Data Collection from Twitter

トレンドマイクロ @trendmicro_jp · 3月10日

【マルウェア「EMOTET」の3月の国内検出台数が1万8,000台を突破し急増中】

2021年11月にポットネットの復活が確認された #EMOTET ですが、国内への攻撃も急増しています。どのような手口を用いて感染を広げるのか、改めてご確認ください。

詳しくは↓ **URL link**

blog.trendmicro.co.jp/archives/30728

16 replies 9 likes

Tweet

Linked website

ホーム > 感染媒体 > メール > 注意！「EMOTET」被害が拡大中

注意！「EMOTET」被害が拡大中 **Title**

投稿日: 2022年3月8日
脅威カテゴリ: メール, スпамメール, 速報, 日本発
執筆: セキュリティエバンジェリスト 岡本 勝之

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。トレンドマイクロの観測では2022年2月の日本国内における総検出台数は18,785件となっており、「最恐ウイルス」とも呼ばれていたテイクダウン前の状況に戻ります。本ブログでもテイクダウン時及び活動再開時に取り上げてまいりましたが、改めてEMOTETの動向について報告いたします。

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)

Title

Text

The screenshot shows the Security NEXT website interface. At the top, there's a navigation bar with categories like 'ニュース' (News), '政府・業界動向' (Government/Industry Trends), '脆弱性' (Vulnerabilities), '製品・サービス' (Products/Services), and 'コラム' (Columns). Below the navigation, there's a sub-header for '[PR] セキュリティニュースのダイジェストを無料メルマガで' (Security News Digest via free email newsletter). The main article title is 「Emotet」感染で従業員装うメール出回る - クラシエ (Emotet infection, employees' emails circulating - Krasie). The article text is highlighted in yellow and contains the following information: Krasie Holdings has confirmed that employees' emails were infected with the Emotet malware, leading to the circulation of phishing emails. The company states that some of its group company's endpoints were infected, and information was leaked, leading to the circulation of phishing emails. The problem email was from a group company employee's name, but the domain was 'kracie.co.jp' instead of the company's actual domain. The company requests that recipients delete the email without opening attachments.

Security NEXTでは、最新の情報セキュリティに関するニュースを日刊でお届けしています。

ニュース 政府・業界動向 脆弱性 製品・サービス コラム

[PR] セキュリティニュースのダイジェストを無料メルマガで

「Emotet」感染で従業員装うメール出回る - クラシエ

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。

同社によれば、グループ会社の一部端末がマルウェア「Emotet」に感染した。情報が流出したと見られ、グループ会社の従業員になりすましたメールが複数送信されていることが確認されているという。

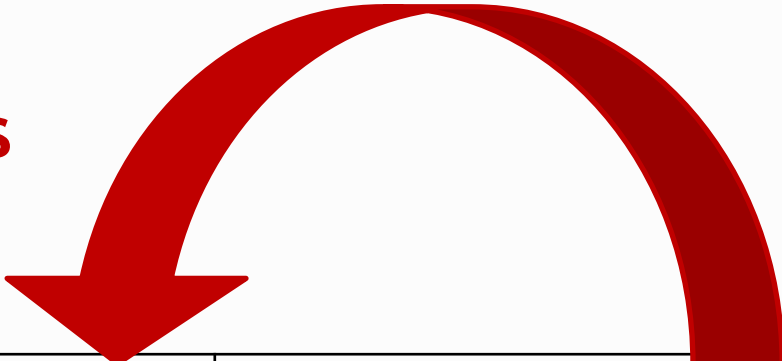
問題のメールは、グループ会社従業員の氏名が表示されているものの、同社ドメイン「kracie.co.jp」とは異なるメールアドレスより送信されていた。

なりすましメールを受信した場合は、添付ファイルを開封せずメールごと削除するよう同社では求めている。

(Security NEXT - 2022/02/18) [ツイート](#)

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

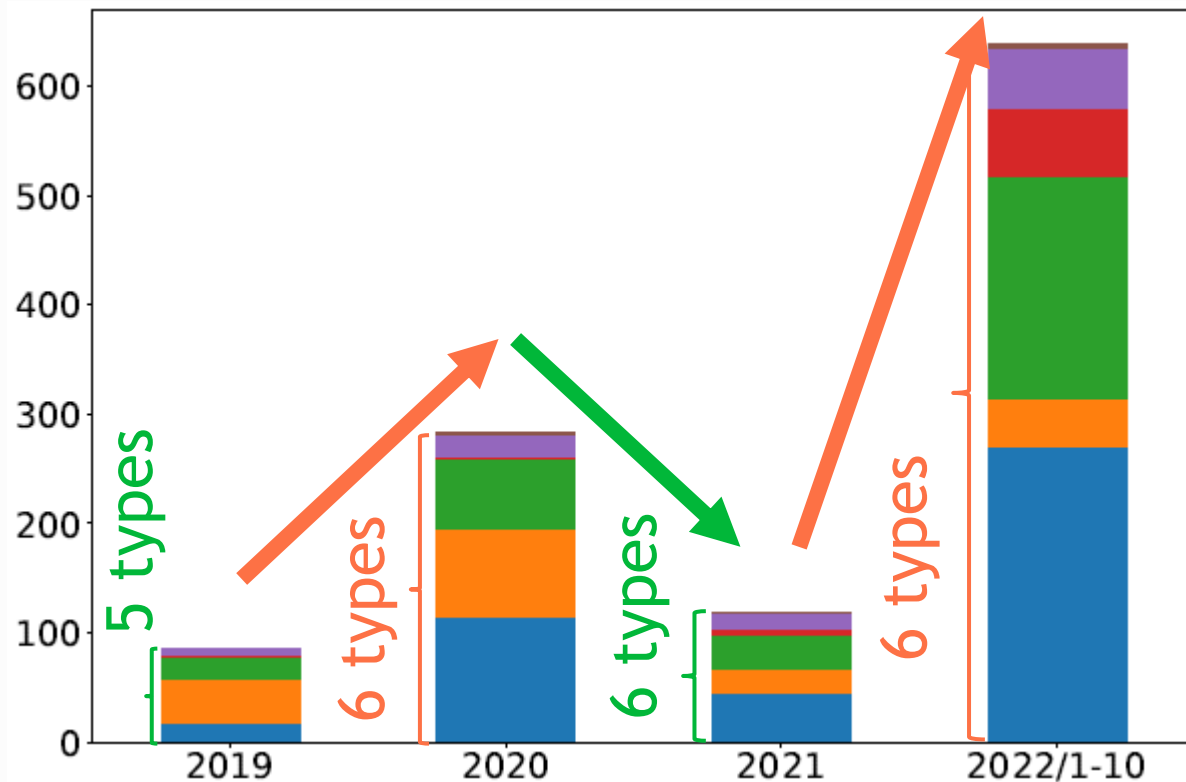


Level of Detail

Malicious File Extension

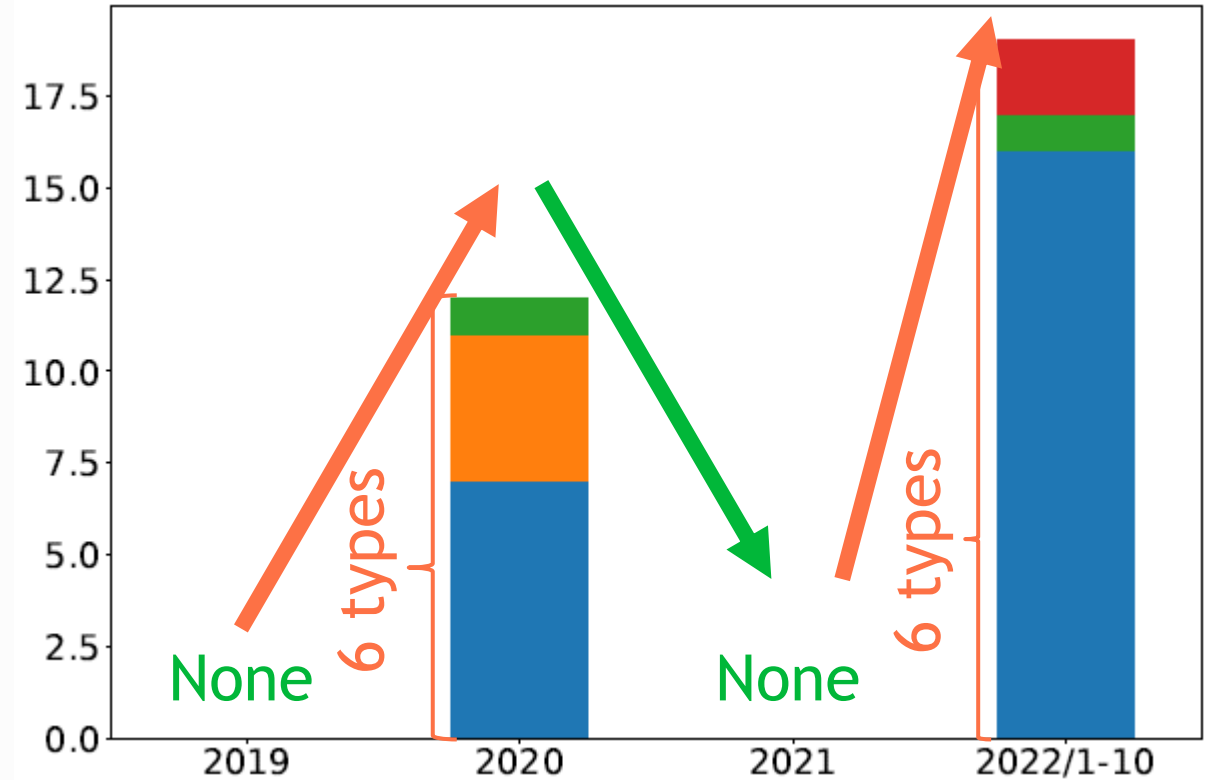
Twitter

- RTF
- XLS
- LNK



Security NEXT

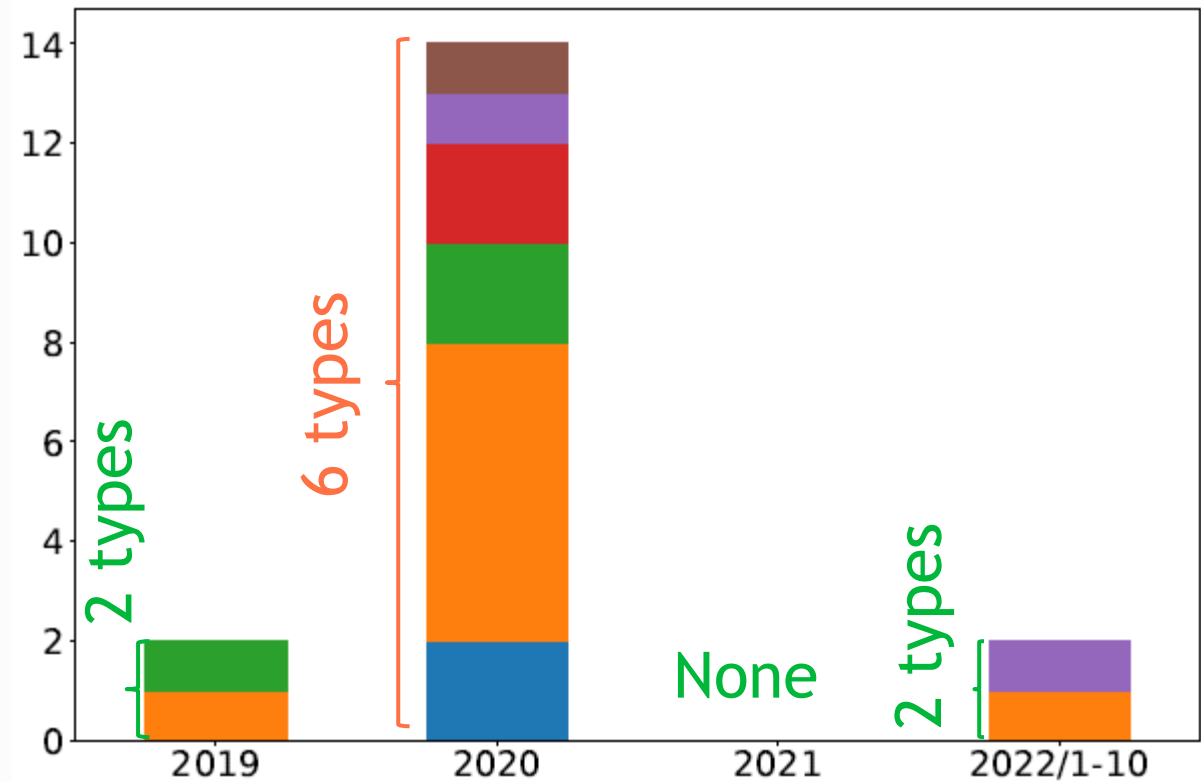
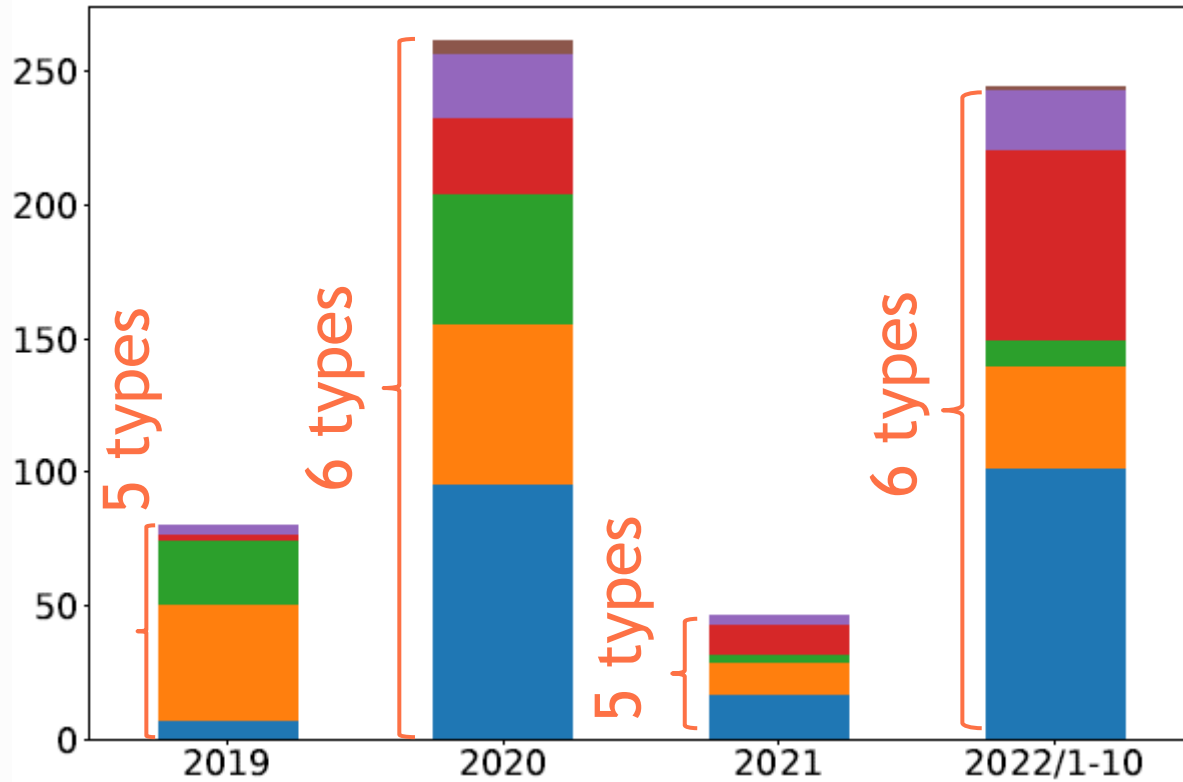
- PDF
- DOC
- ZIP



Twitter

Security NEXT

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

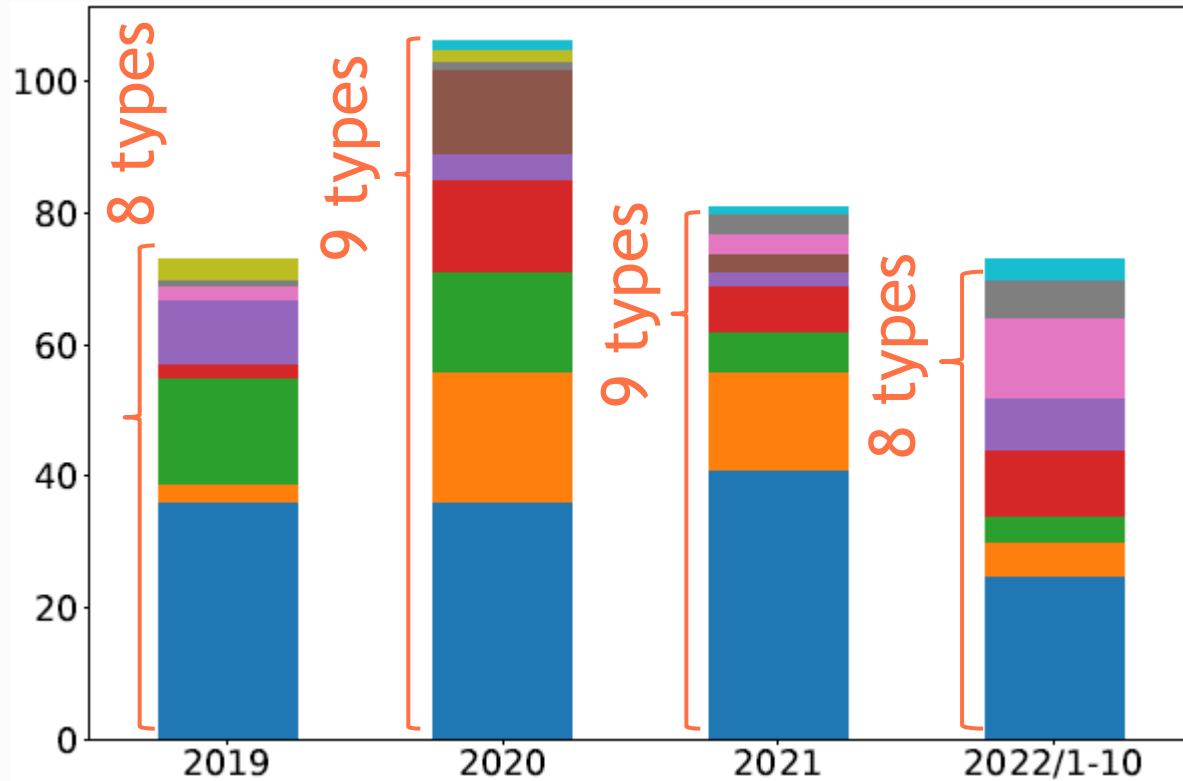


Level of Detail

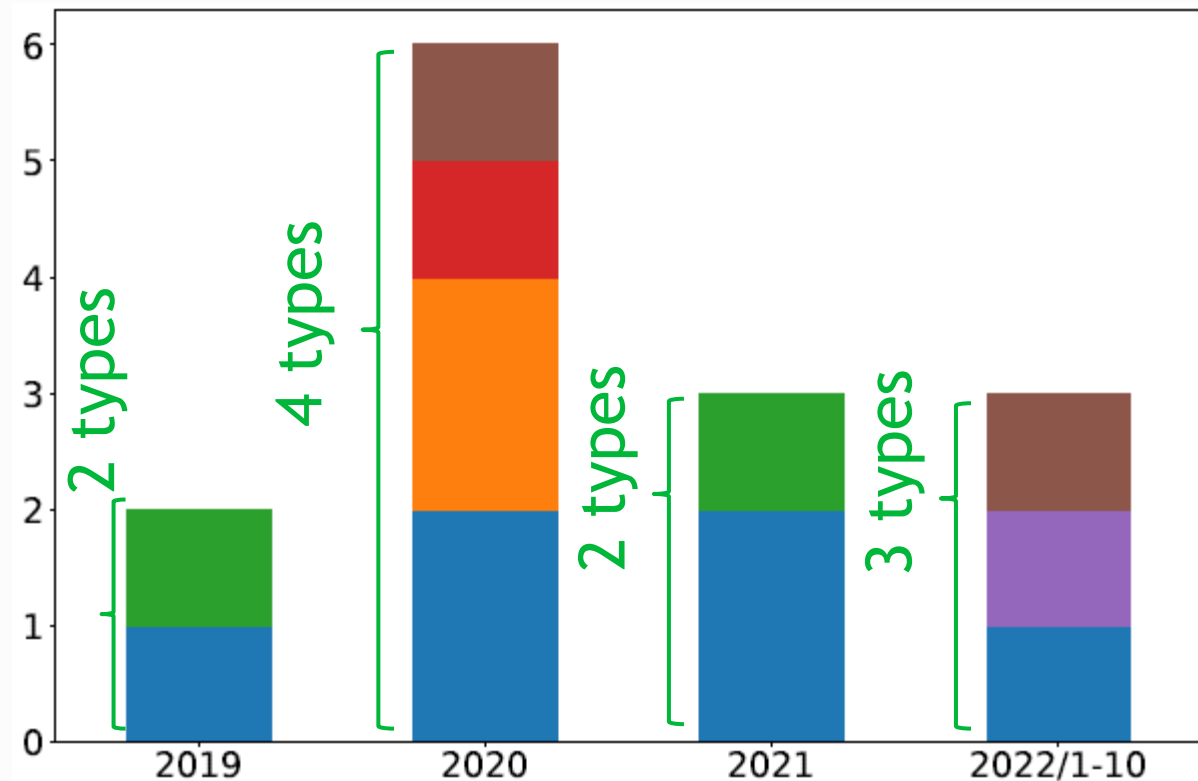
Malware Distributed by Emotet

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

Twitter



Security NEXT



Comparison Method

■ Level of detail



■ Real-time performance

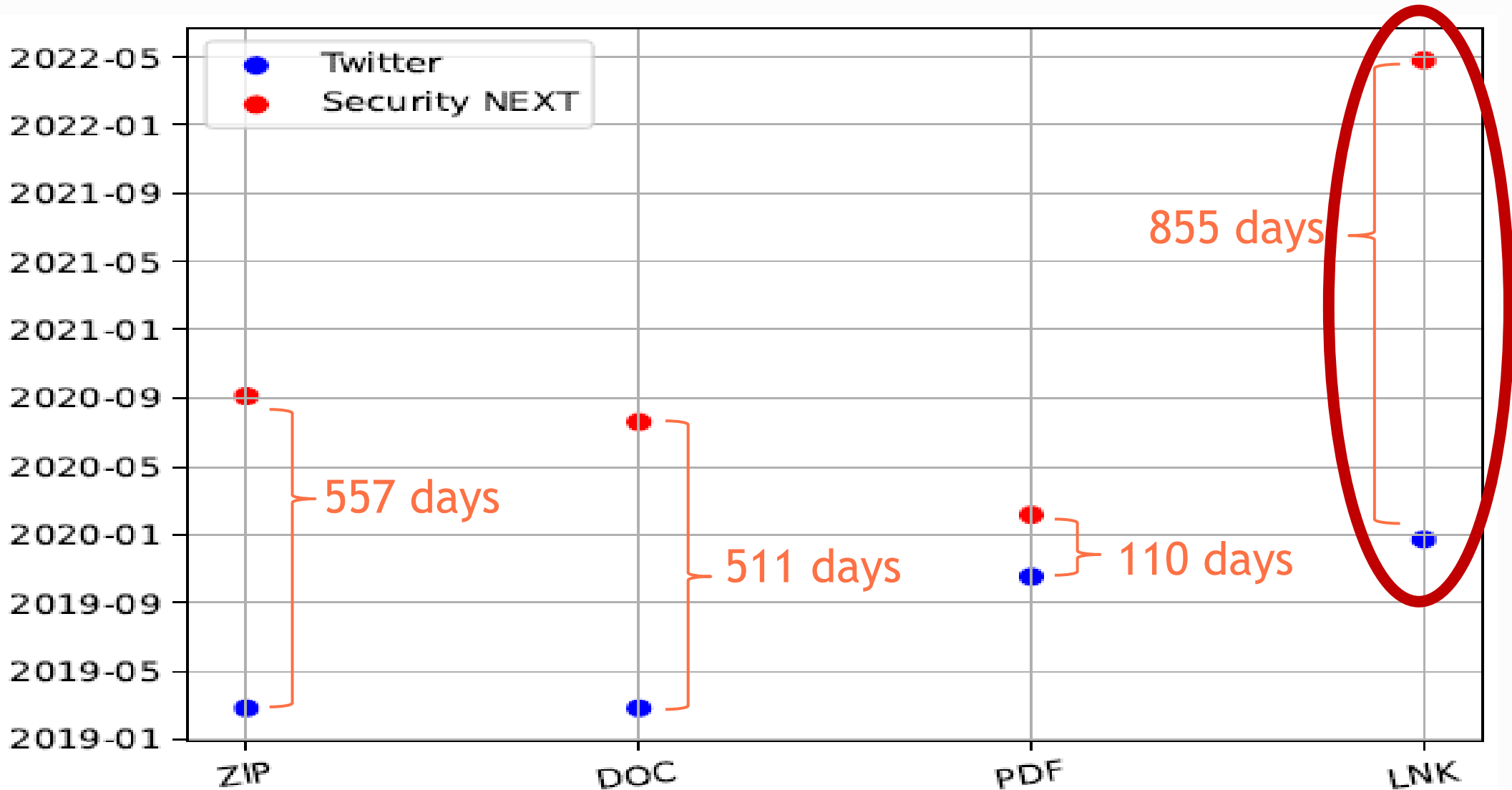


■ Reliability



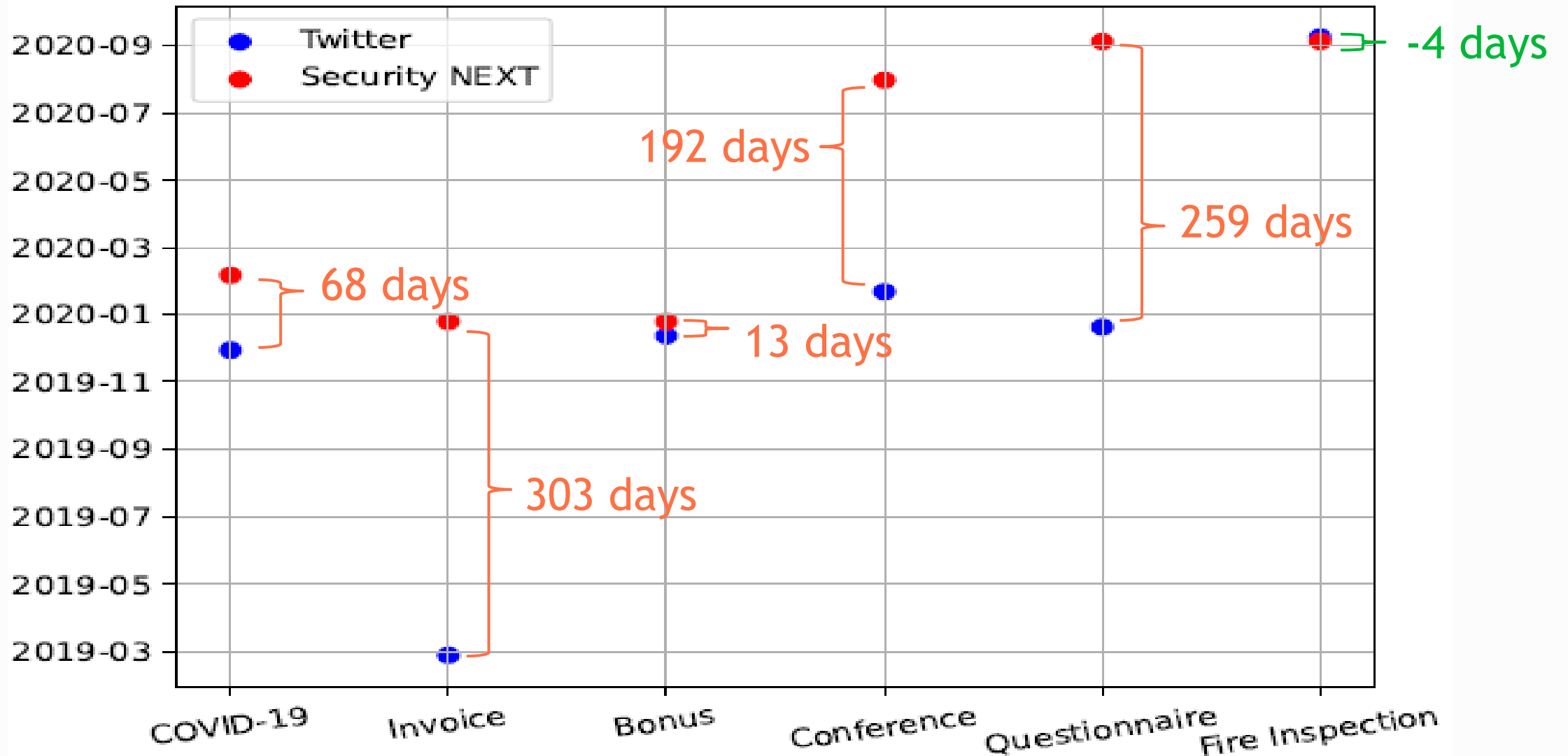
Real-time Performance

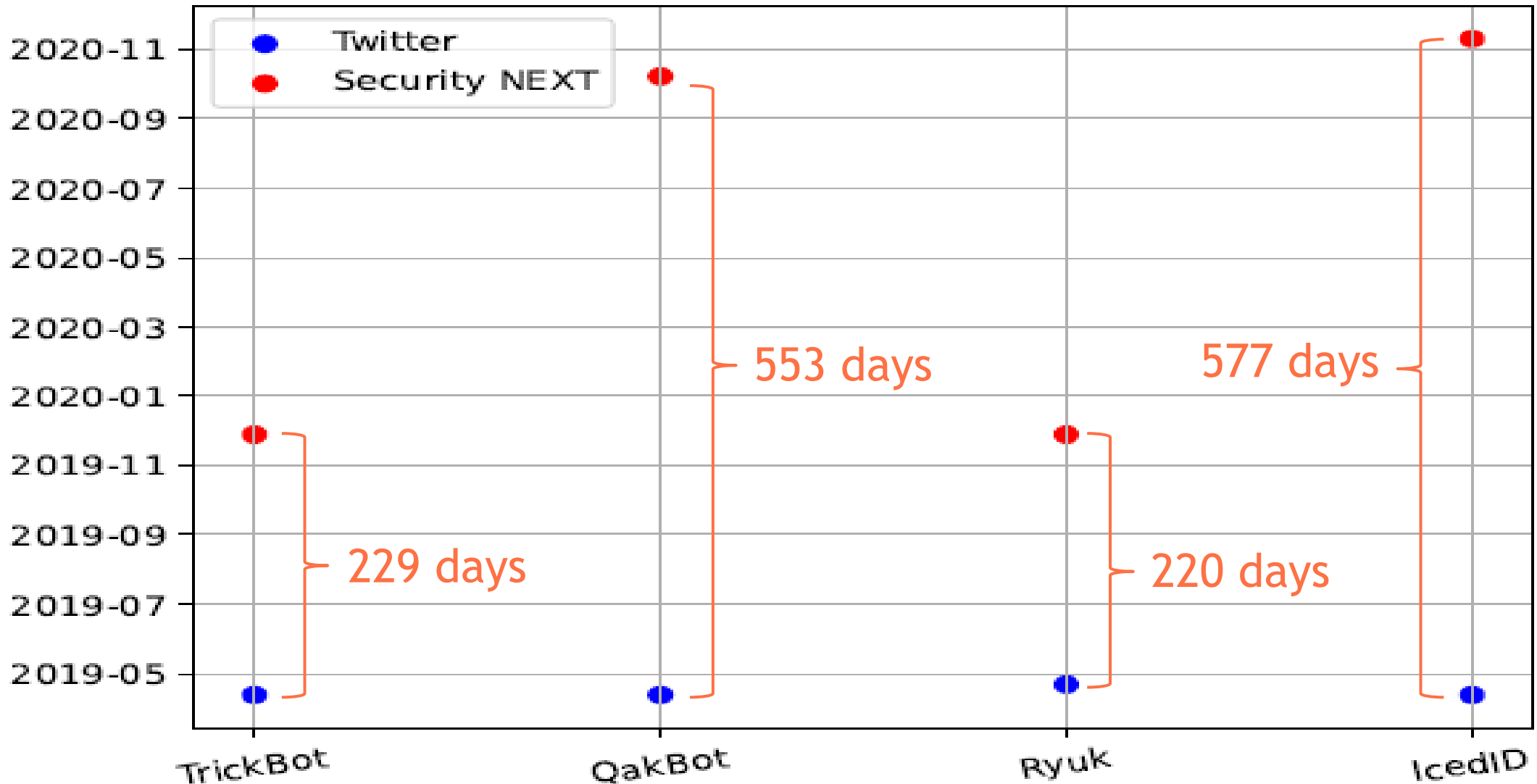
Malicious File Extension



Real-time Performance

Spam Email Subject Line



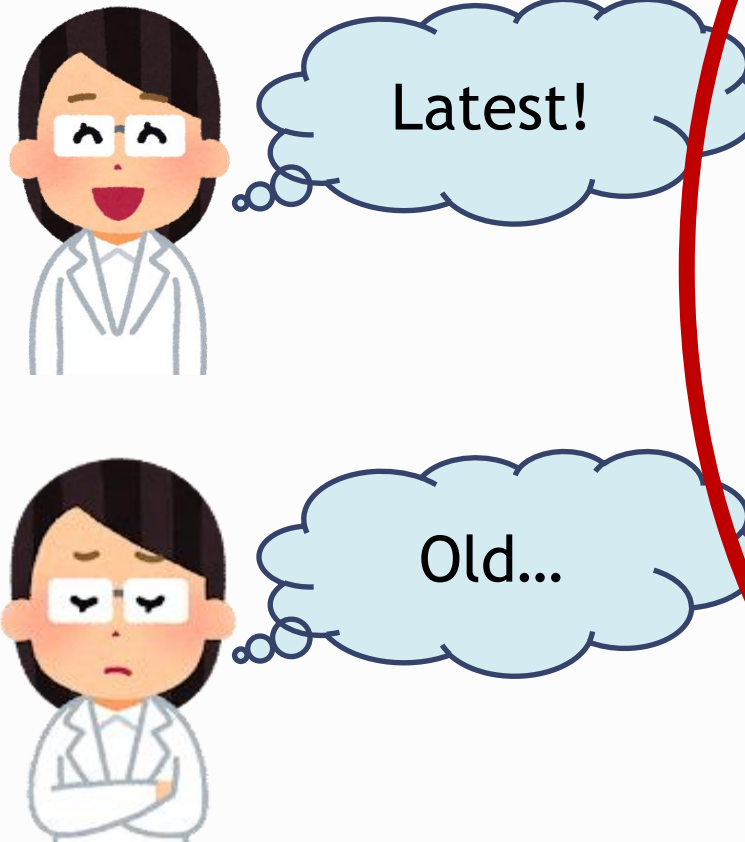


Comparison Method

■ 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	<u>Published or updated date</u>	20 / 20	20 / 20
4	SSL certificate	20 / 20	20 / 20
5	<u>Sources with links</u>	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	Twitter	>>	Security NEXT	Twitter	≈	Security NEXT
Malicious file extension			Malicious file extension			Total score		
5 ~ 6 types		0 ~ 6 types	Publish delay		110 ~ 855 days	113 / 160		141 / 160
Spam email subject line			Spam email subject line			Sources with links		
5 ~ 6 types		0 ~ 6 types	Publish delay		-4 ~ 303 days	14 / 20		1 / 20
Malware distributed by Emotet			Malware distributed by Emotet			No link errors		
8 ~ 9 types		2 ~ 4 types	Publish delay		220 ~ 577 days	8 / 20		20 / 20

Thank you for your attention!