

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

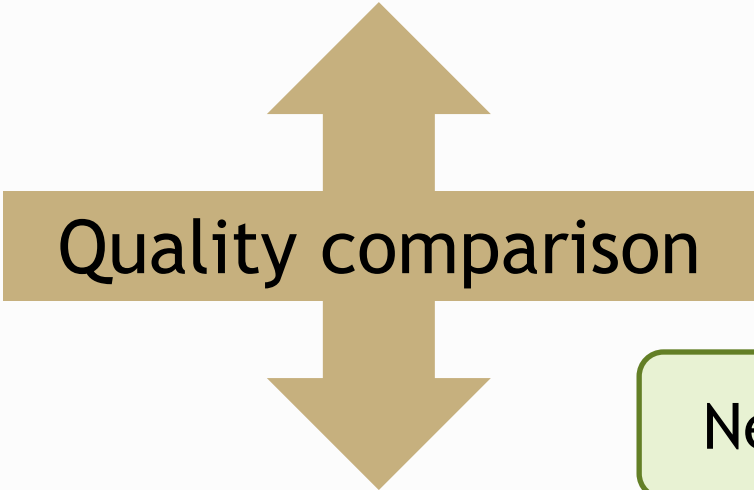
<https://ieeexplore.ieee.org/abstract/document/9527964>

Alerting security experts to potential threats

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

Case Study

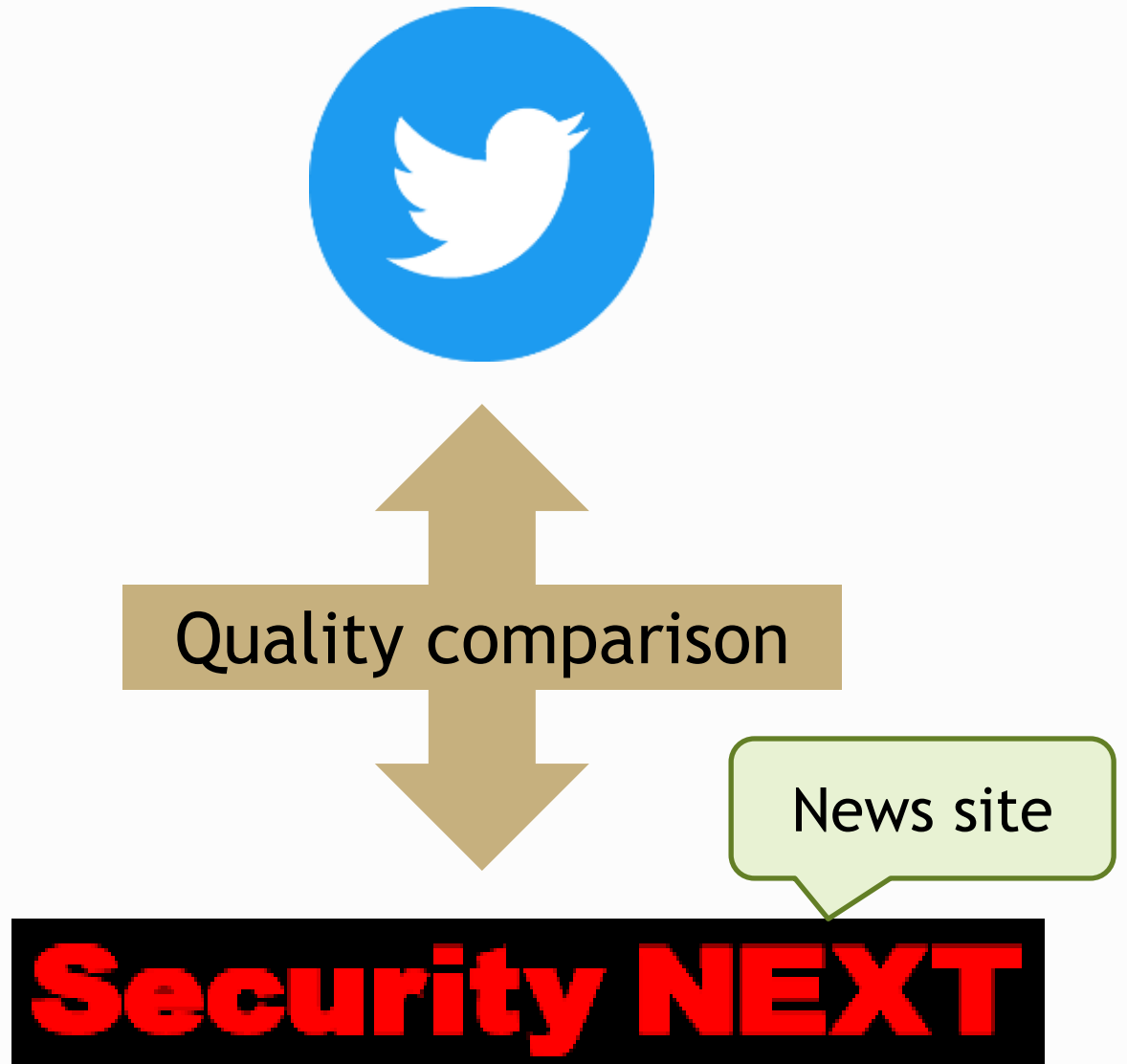
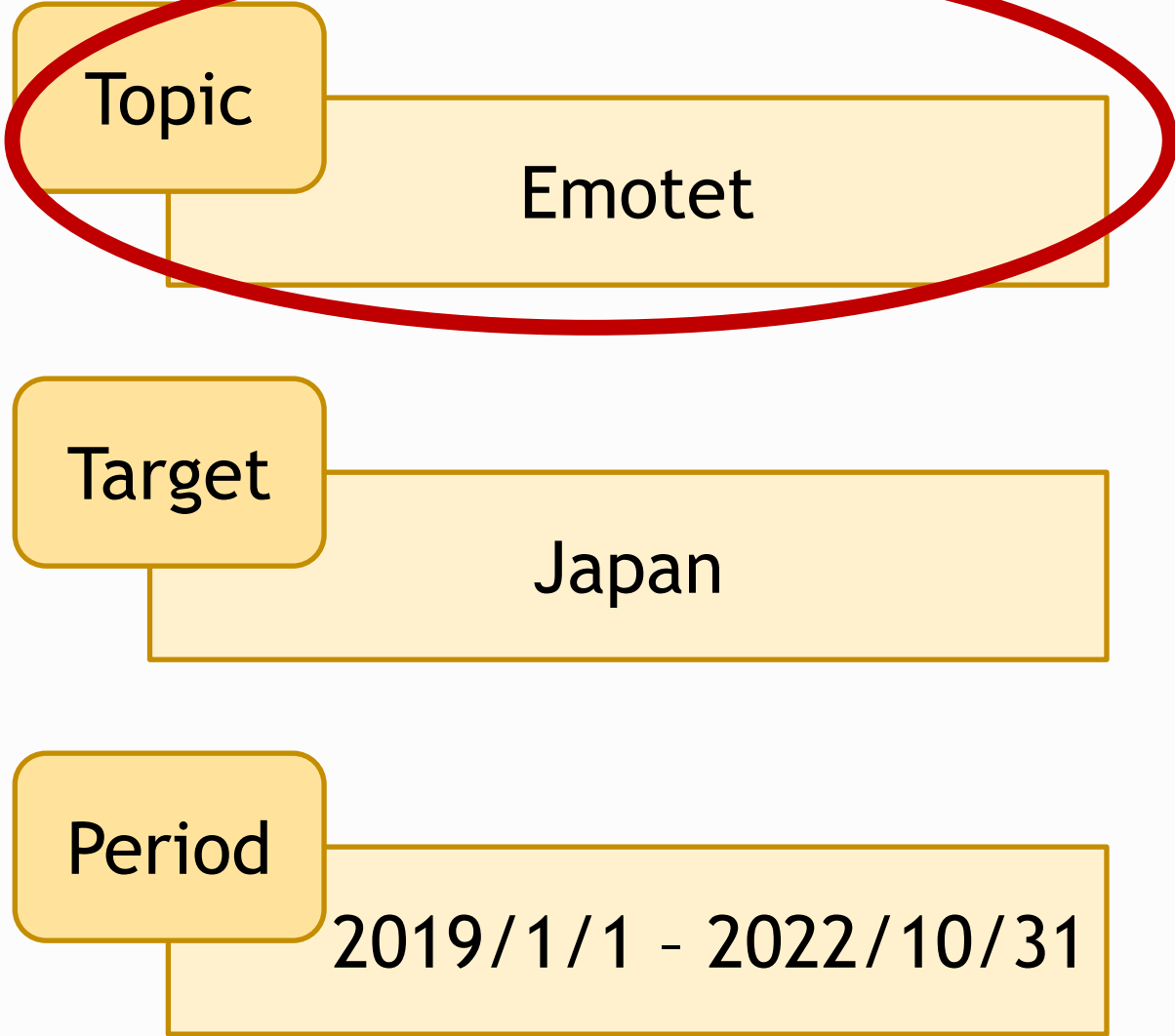
Topic	Emotet
Target	Japan
Period	2019/1/1 - 2022/10/31



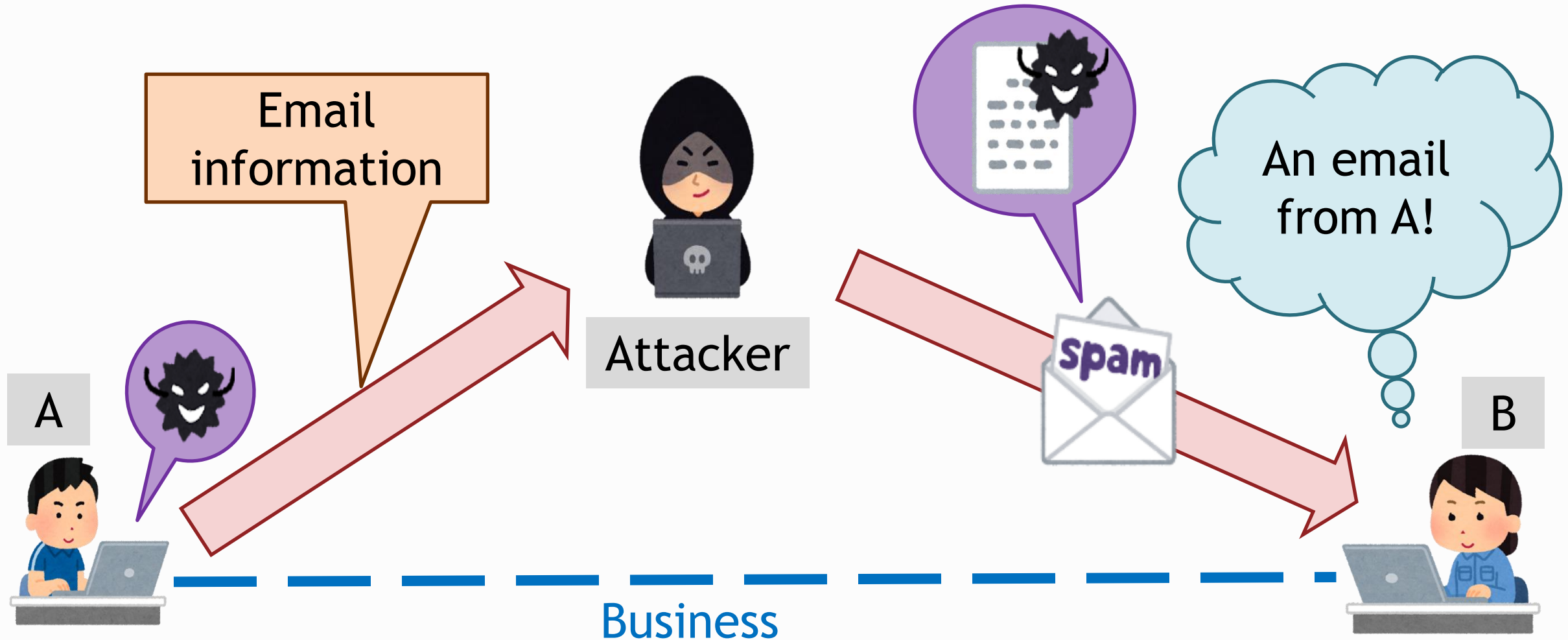
News site

Security NEXT

Case Study



Emotet

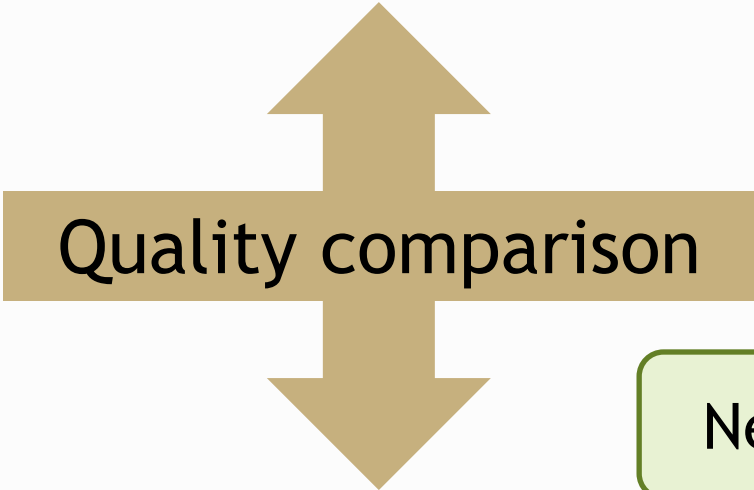


Case Study

Topic: Emotet

Target: Japan

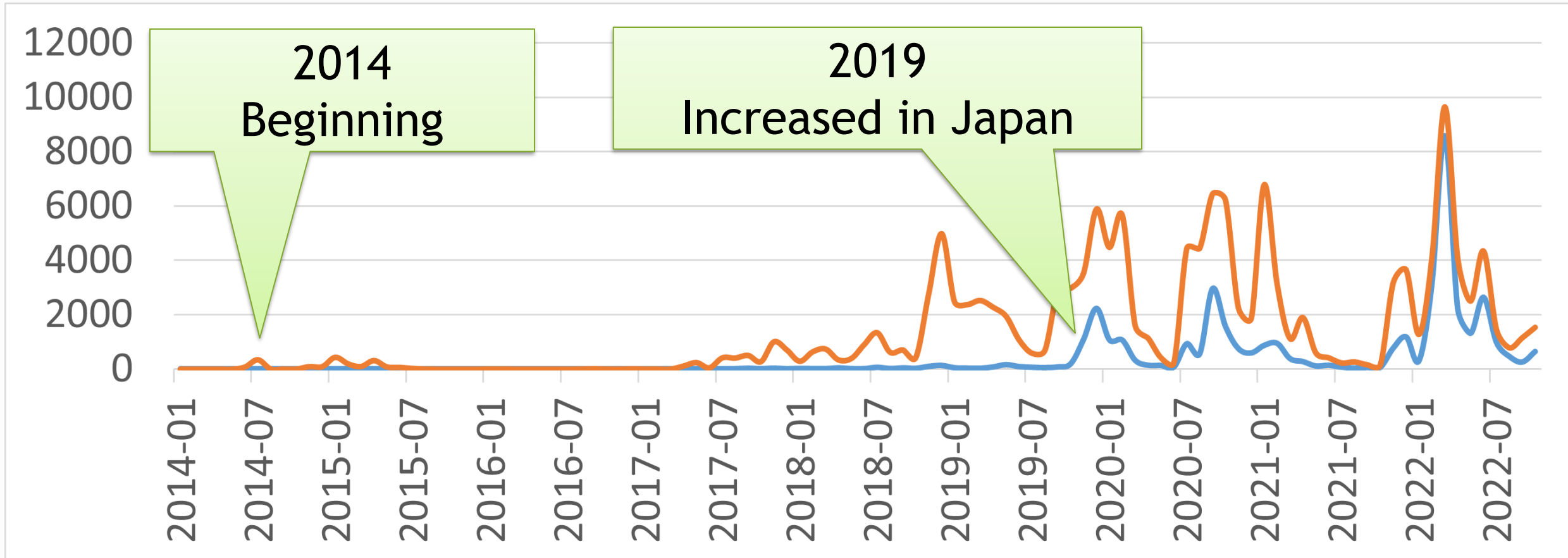
Period: 2019/1/1 - 2022/10/31



Security NEXT

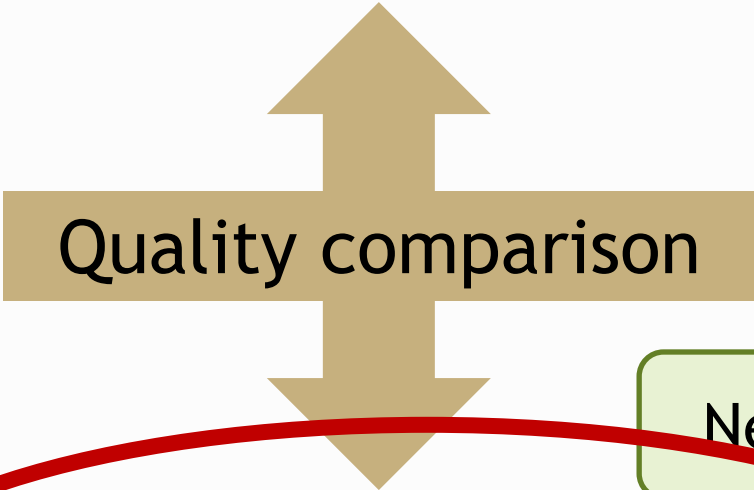
Emotet Tweets

- 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

Security NEXT Security NEXTでは、最新の情報セキュリティに関するニュースを毎日お届けしています。 Google 提供 検索

社会人・大学生向け英語講座 すべて使えて ¥3,480/月 Asteria for business Z会公式サイト

ニュース 政府・業界動向 脆弱性 製品・サービス コラム 過去記事 メルマガ

[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

ニュース関連記事の一覧 (1ページ目 / 全978ページ)

- 2022/11/01 [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 [メール転送エージェント「Exim」のDMARC関連処理に脆弱性](#)
- 2022/10/31 [深い脆弱性へ対処した「OpenSSL 3.0.7」が11月1日に公開予定](#)
- 2022/10/31 [幼稚園の入園願書など紛失、マイナンバー記載 - 京田辺市](#)
- 2022/10/31 [研修申込者の個人情報をネット上に誤公開 - 埼玉県](#)
- 2022/10/31 [じゃらん.net装うフィッシング攻撃が発生 - 全国旅行支援を憂るか](#)
- 2022/10/31 [RPCフレームワーク「Apache Dubbo」に深刻な脆弱性](#)
- 2022/10/28 [「VMware Cloud Foundation」の深刻な脆弱性、悪用コードが公開](#)
- 2022/10/28 [「Chrome」にゼロデイ脆弱性 - アップデートが公開](#)
- 2022/10/28 [ゼロデイ脆弱性も解消した「iOS 15.7.1」「iPadOS 15.7.1」をリリース - Apple](#)
- 2022/10/28 [「サイバーセキュリティ経営ガイドライン Ver3.0」の意見募集が開始に](#)
- 2022/10/28 [印刷通販サイトに不正アクセス - クレカ情報など流出した可能性](#)
- 2022/10/28 [イベント当選者のメアド流出、一斉送信機能に不具合 - アニメイトカフェ](#)

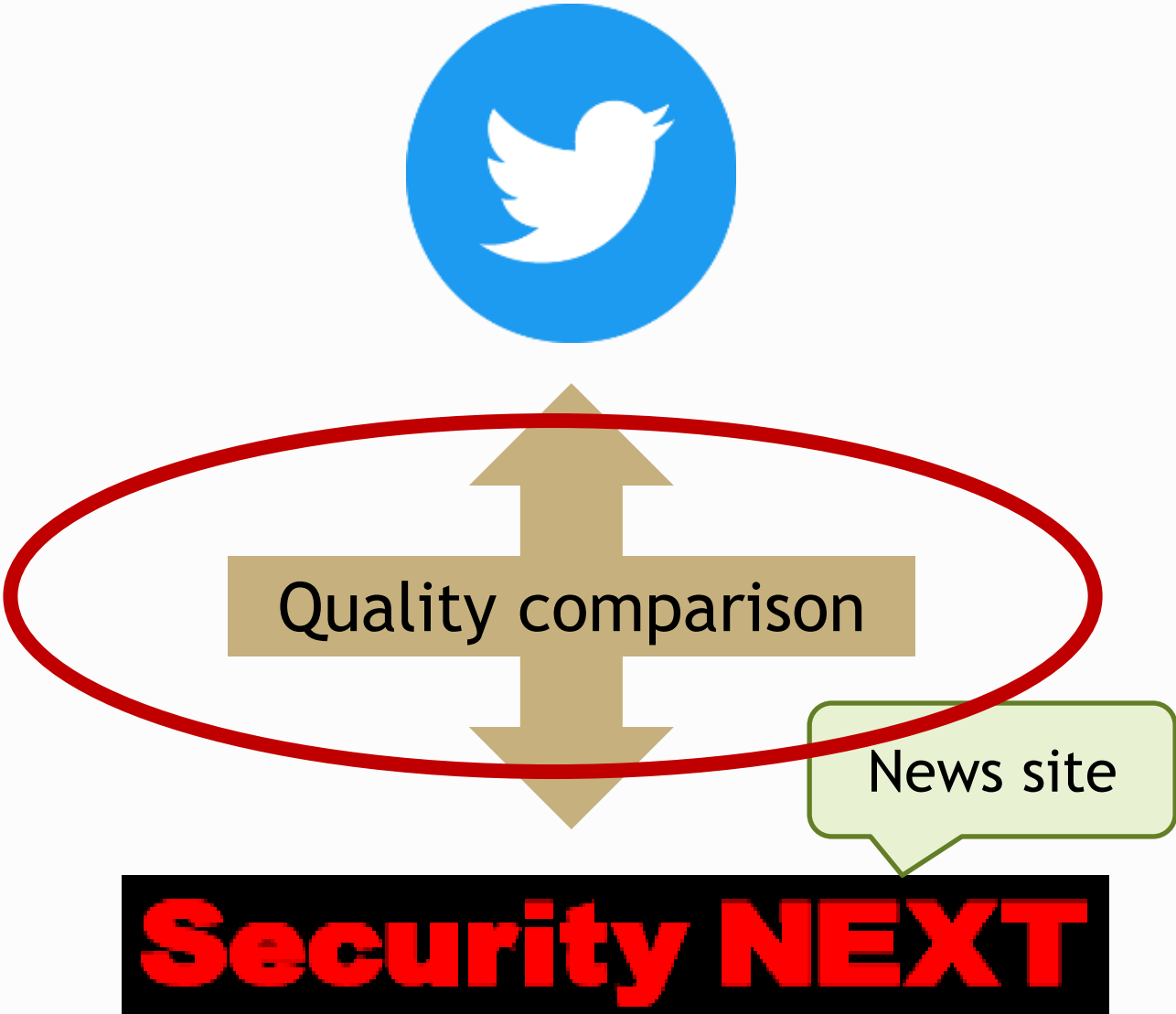
年、売れてます! 40~60代の会社員必読! この本を読まずに 年金を受給したら後悔する! 結局、年金は何歳でもらうのが一番トクなのかな? 事業変革を推進するための最新技術とつながる総合展 EdgeTech+ 2022 11月16日(水)~18日(金) パシフィック横浜

Z-KAI TOEIC対策講座 Adaptive AI搭載・講義付き お申し込み特典 「スコアUP・学習Tips」掲載特別冊子 公式ページへ

ピックアップ 深刻な脆弱性へ対処した「OpenSSL 3.0.7」が11月1日に公開予定 下請へのセキュリティ要請、問題なし - ただし層別的地位の適用となるケースも 「VMware Cloud Foundation」の深刻な脆弱性、悪用コードが公開 「Chrome」にゼロデイ脆弱性 - アップデートが公開 「サイバーセキュリティ経営ガイドライン Ver3.0」の意見募集が開始に 「VMware Cloud Foundation」に深刻な脆弱性 - OSSの既知脆弱性に起因 Apple、「iOS 16.1」「iPadOS 16」を公開 - ゼロデイ脆弱性を修正 ウェブの利便性高めるSaaSが改ざん被害 - 導入サイトで情報窃取のおそれ 2022年3Qの脆弱性届け出、ソフトとサイトのいずれも増加

Case Study

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

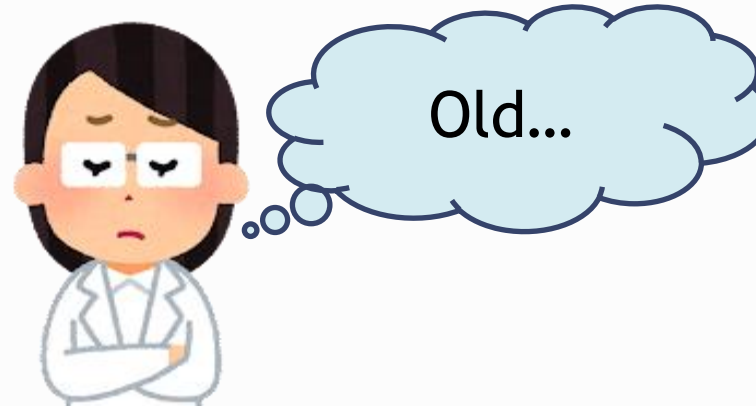


Comparison Method

■ 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)

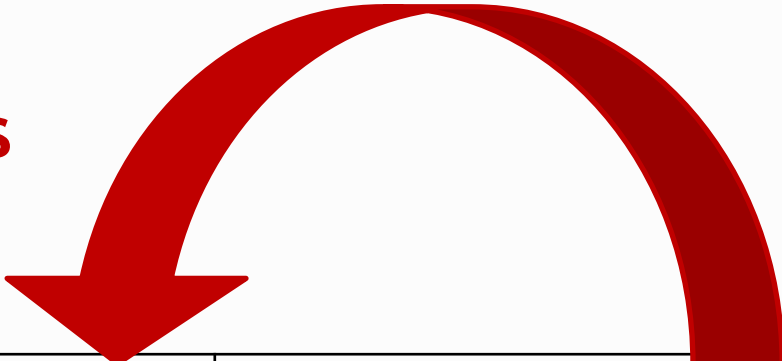
Title

Text

The screenshot shows the Security NEXT website interface. At the top, the logo 'Security NEXT' is displayed in red, followed by a tagline: '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。' Below this is a navigation bar with categories: 'ニュース', '政府・業界動向', '脆弱性', '製品・サービス', and 'コラム'. A sub-header reads: '[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'. The main article title is '「Emotet」感染で従業員装うメール出回る - クラシエ', where 'Emotet' is underlined in red and the entire title is enclosed in a green box. The article text is enclosed in a yellow box and contains several underlined phrases: '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。', '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。', and '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。'. At the bottom of the article, there is a date '(Security NEXT - 2022/02/18)' and a 'ツイート' (Tweet) button.

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

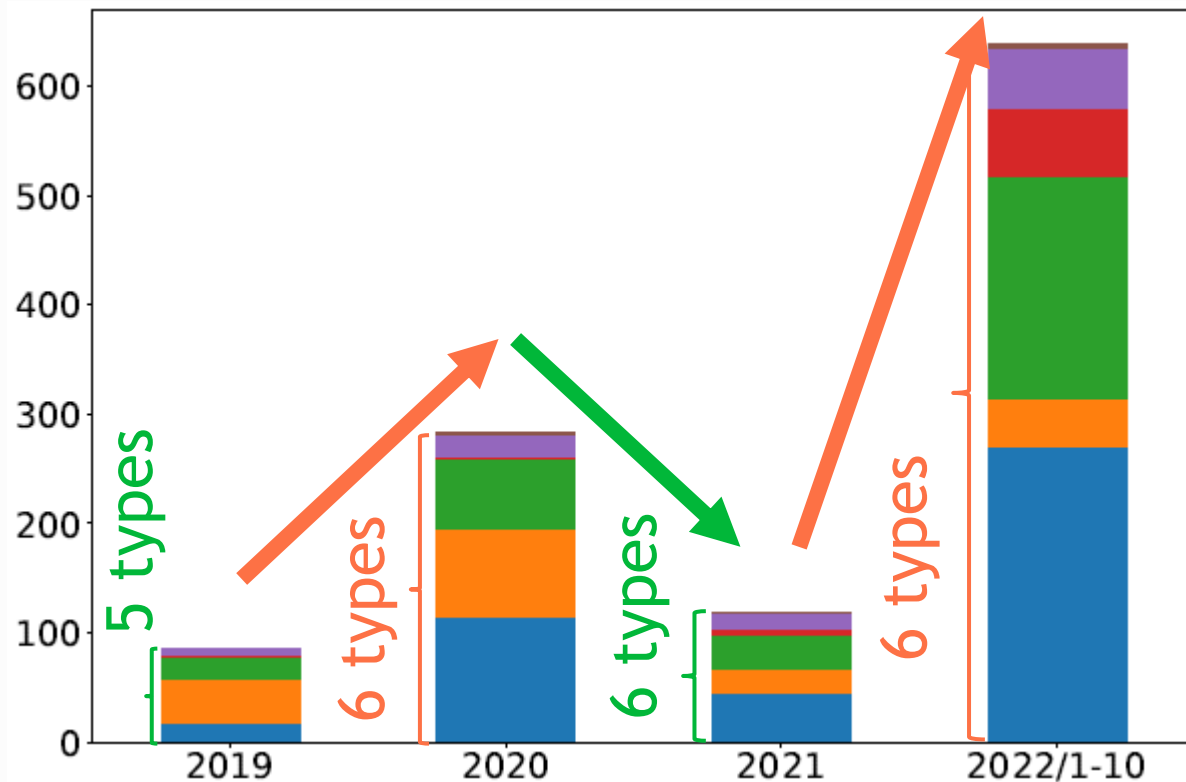


Level of Detail

Malicious File Extension

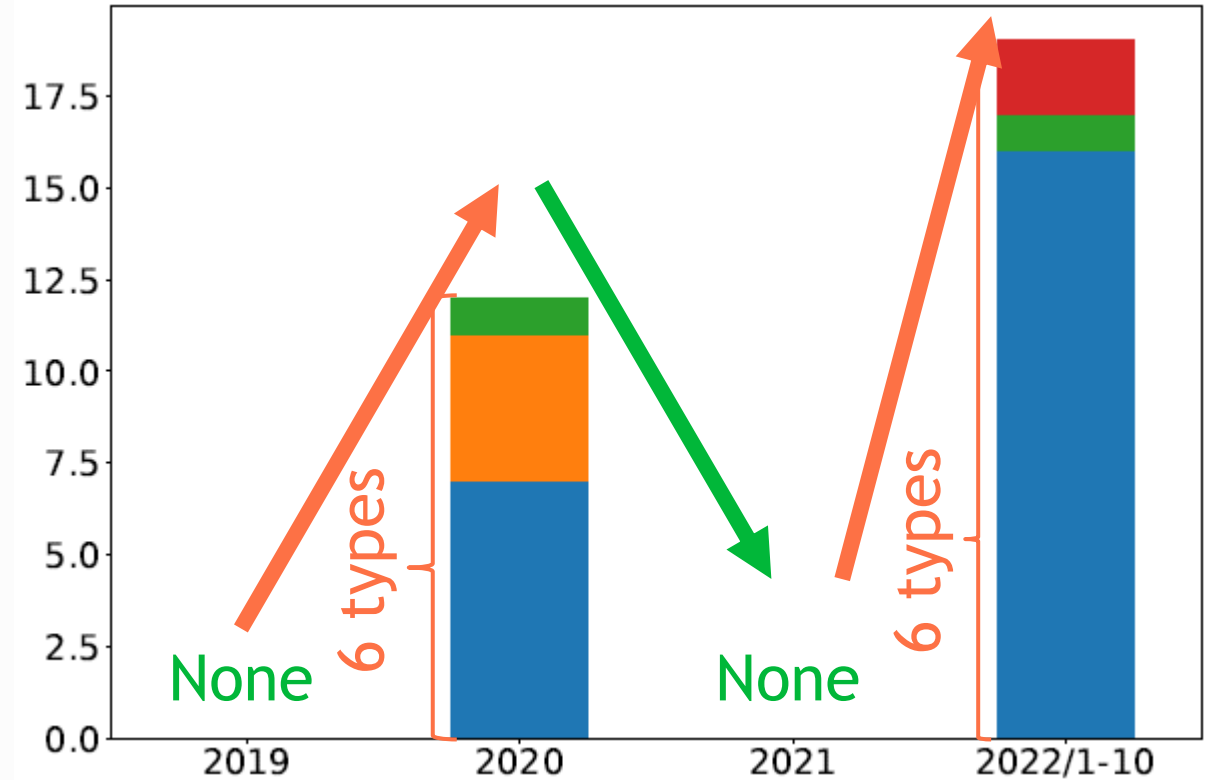
Twitter

- RTF
- XLS
- LNK



Security NEXT

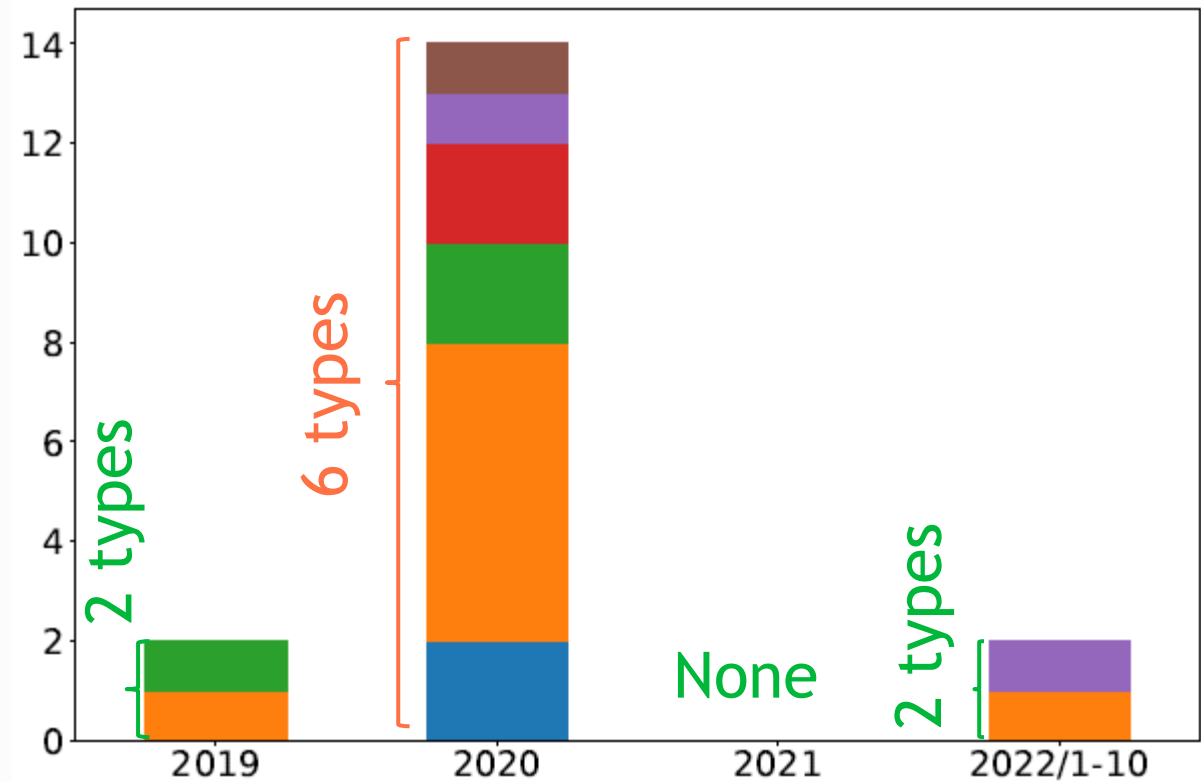
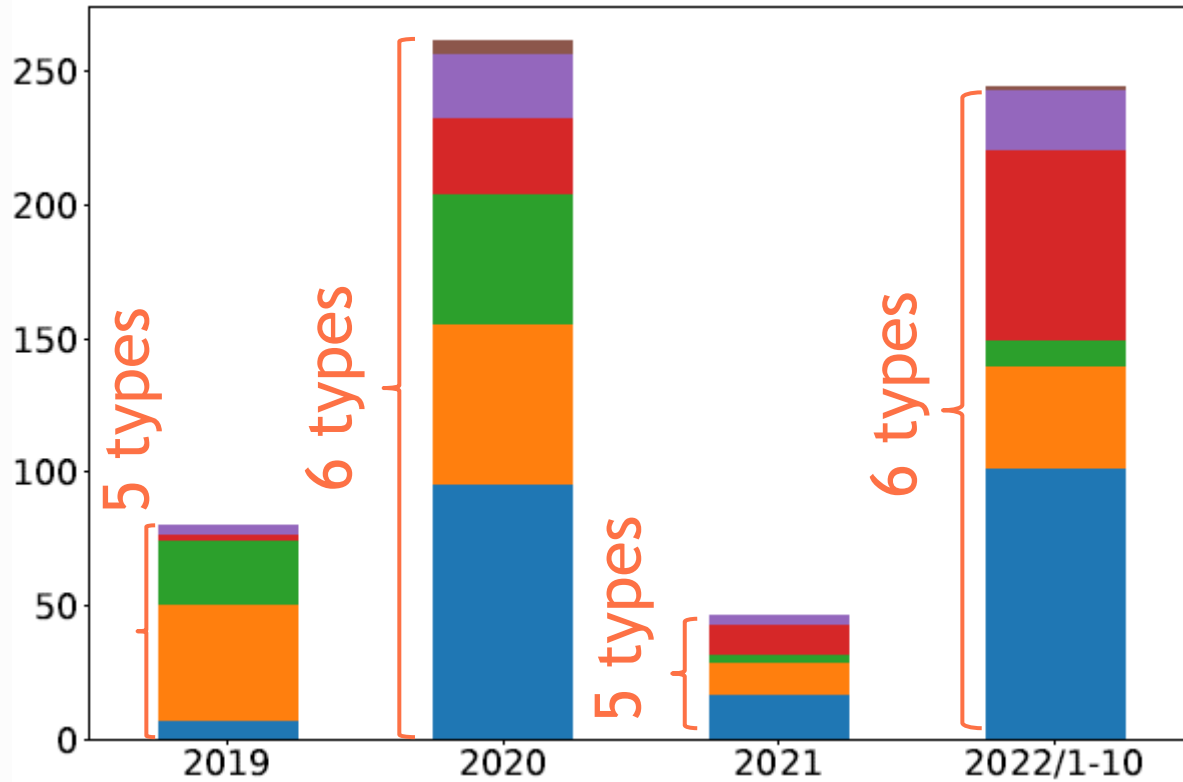
- PDF
- DOC
- ZIP



Twitter

Security NEXT

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

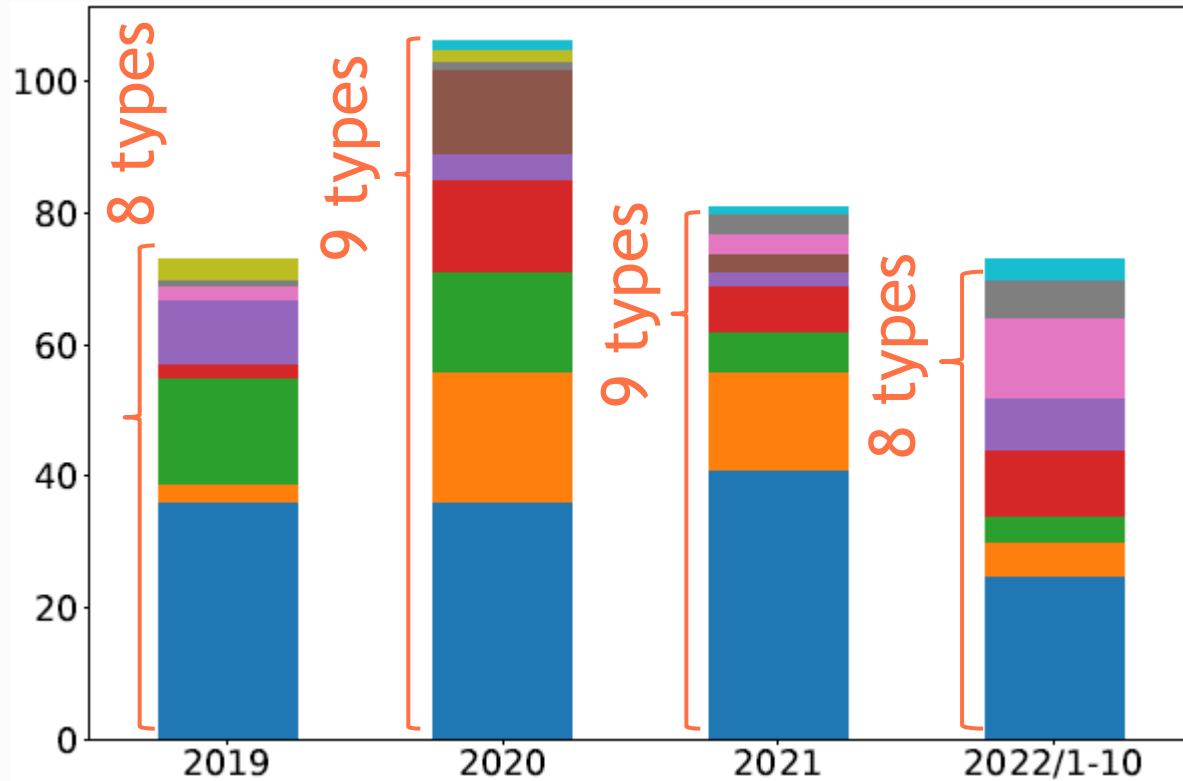


Level of Detail

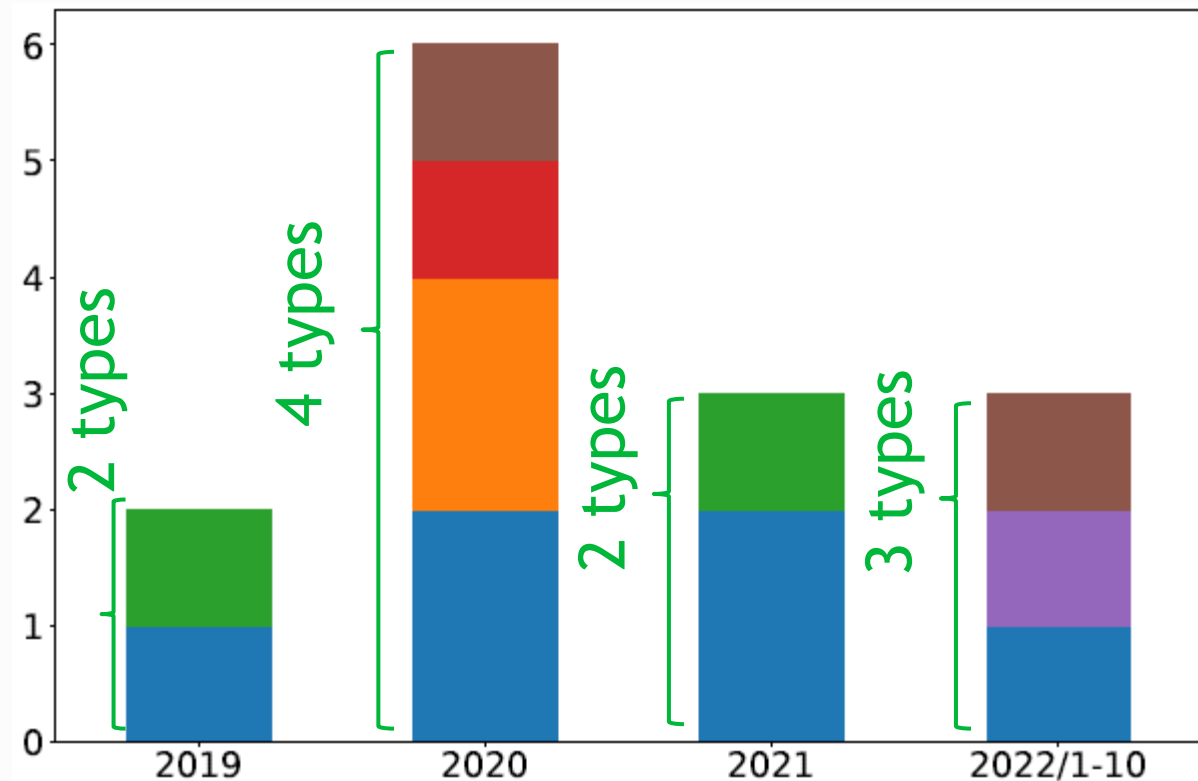
Malware Distributed by Emotet

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

Twitter



Security NEXT



Comparison Method

■ Level of detail



■ Real-time performance

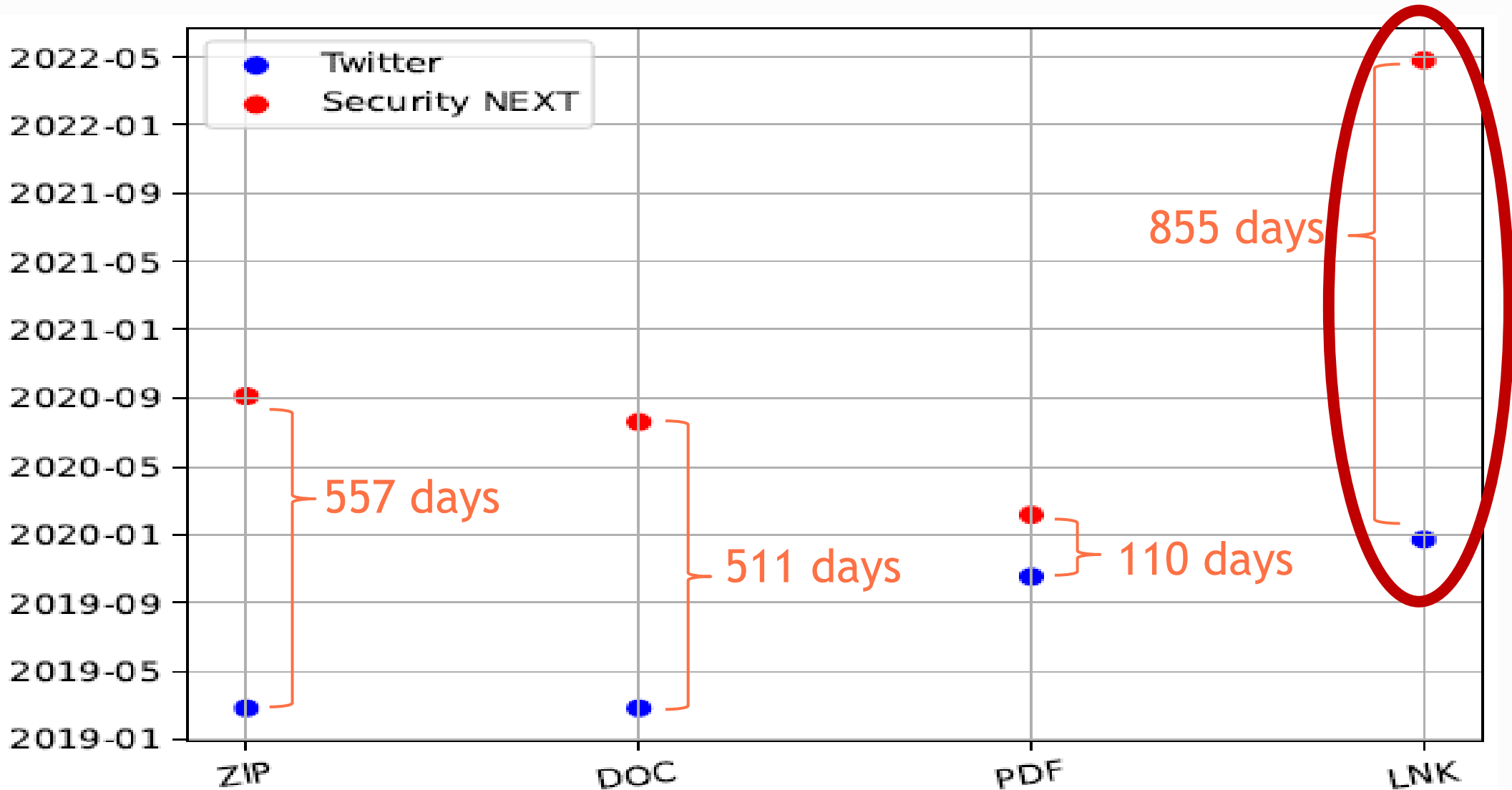


■ Reliability



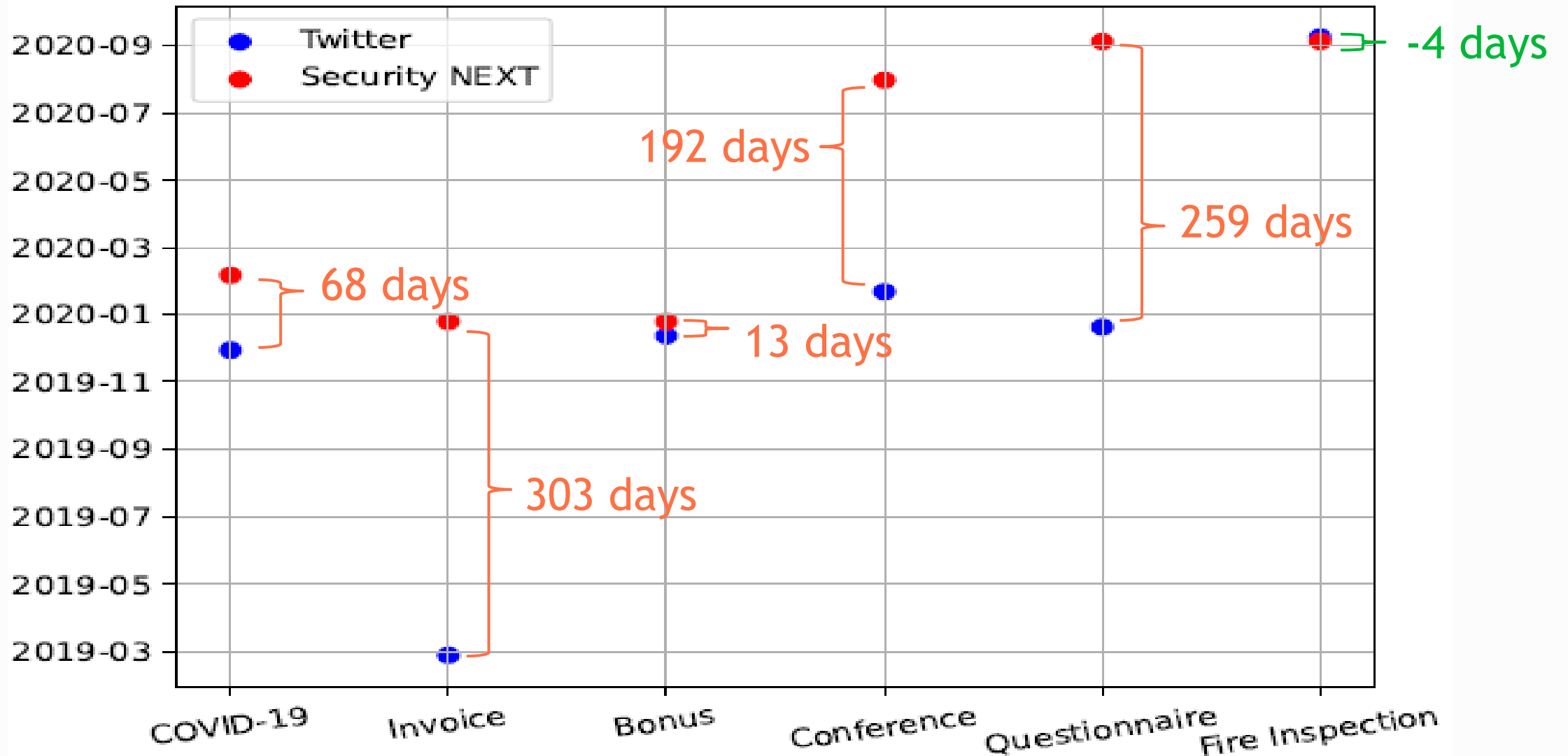
Real-time Performance

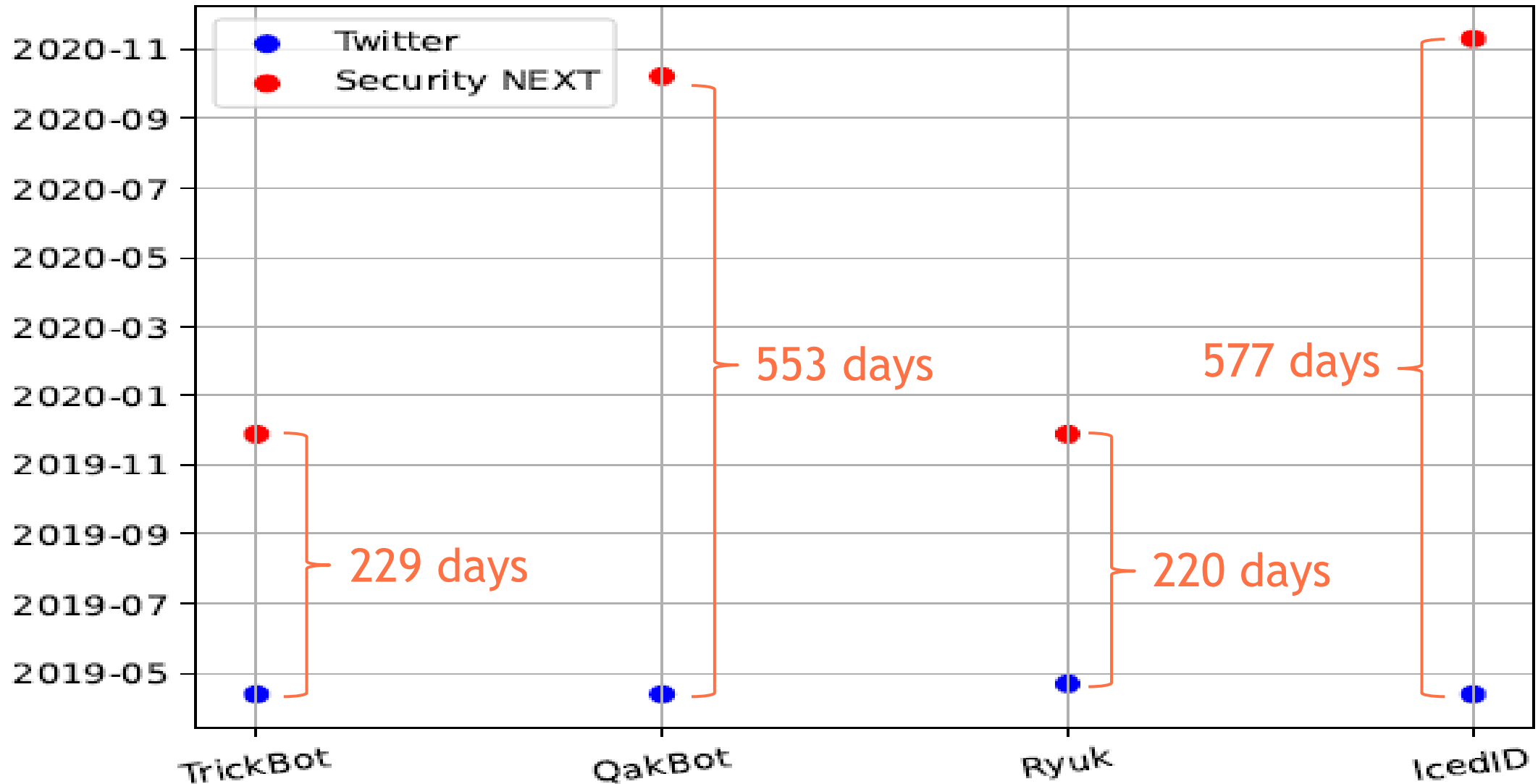
Malicious File Extension



Real-time Performance

Spam Email Subject Line



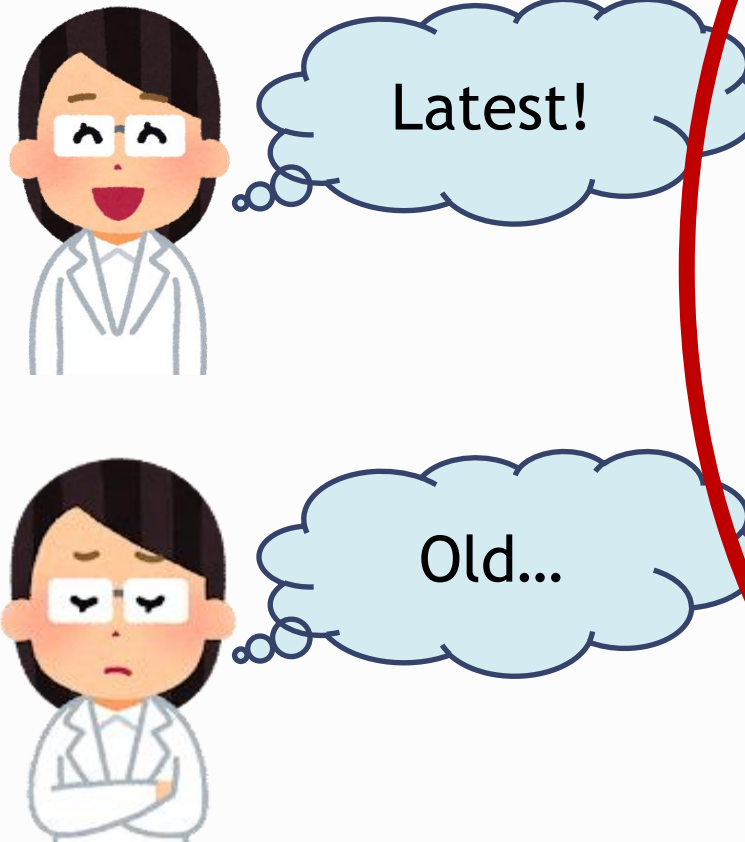


Comparison Method

■ 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!