

# Exploring Cybersecurity Research at SecureBrain

Kazuki TAKADA Ph.D.

SecureBrain Corporation.

November 29, 2023 - December 01, 2023

8th Franco-Japanese Cybersecurity Workshop

# SecureBrain Corporation

Office	Kioicho Building 7F, 3-12 Kioicho, Chiyoda-ku, Tokyo, JAPAN
Founded	October 5, 2004
Representative	Nobutoshi Sagawa, President and CEO
Business	1) Cybersecurity solutions 2) Cybercrime Incident Response 3) Cybersecurity SDK and OEM 4) Research, analysis, and development on cybercrime and their countermeasures
Capital	251.8 million yen (approx. USD 2 million)
Share Holder	Hitachi Systems Ltd (Acquired Oct 2014)

Protecting your business from Cybercrime.

# Table of Contents

## A) Development of Remote & Automatic IoT Malware-Disabling Technology

- Background
- IoT malware-disabling technology
  - IoT malware-disabling information automatic extraction system
  - IoT malware-disabling system
  - Evaluation
- Large-scale IoT simulator
- Conclusion

## B) For Reduction of Phishing Scam

- PhishWall
- Scam Radar BD

# Development of Remote and Automatic IoT Malware-Disabling Technology

This research was conducted under a contract of "Research and development on IoT malware removal / make it non-functional technologies for effective use of the radio spectrum" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan.

# Background

Internet traffic by cyber-attacks has been increasing over the past several years.

There is a large amount of traffic by internet-of-things(IoT) infected malware(IoT malware) among them.

The IoT devices used in a particular use case cannot be stopped or suspended for maintenance.

Mirai is one of the known malwares.

Mirai has malicious functions such as

- The ability to crawl and infect a large number of IoT devices.
- Transmitting a large amount of communication to cause Distributed Denial of Service (DDoS) attacks

# Research objective

We have proposed disabling IoT malware by leveraging its vulnerabilities or functions.[1][2]

This study aims to develop the IoT malware-disabling technology based on previously proposed concept.

The IoT malware-disabling technology aims to remotely and automatically disable IoT malware without disrupting the activities of the IoT devices.

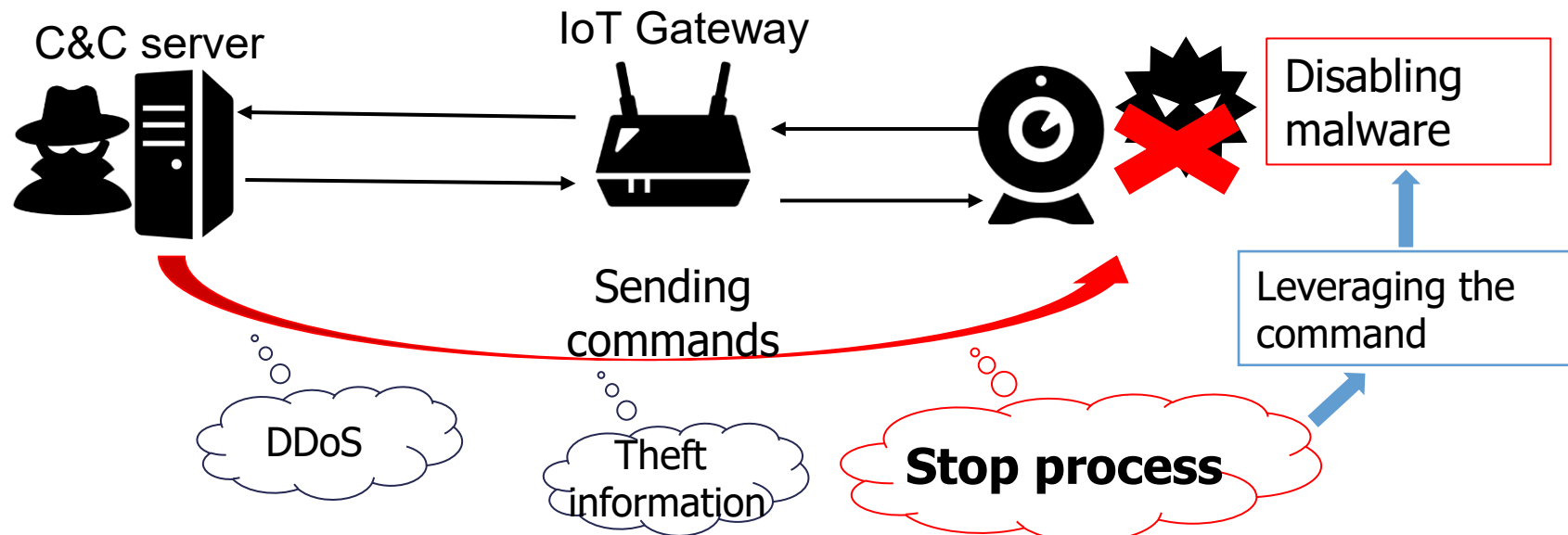
We also develop the large-scale IoT simulator to comprehensively evaluate the effects of the IoT malware-disabling technology.

[1] Takeshi Misu, Tatsuaki Momoi, “Proposal of IoT malware removal method using dummy C&C server,” 2019 Symposium on Cryptography and Information Security(SCIS 2019), 3E2-2, IEICE, Jan. 2019.

[2] Takeshi Misu and Kazuki Takada, “Investigation of IoT malware disablement method using dummy C&C server,” IPSJ SIG Technical Report, Vol.2019-CSEC-86, No.9, pp.1–7, Information Processing Society of Japan, July 2019.

# Concept of our technology

- Almost IoT malware (like Mirai, Bashlite) communicates with Command and Control (C&C) server.
- Attackers operate the IoT malware via the C&C servers by sending various commands.
- We found to be able to disable the IoT malware by sending disabling information (like kill-command) from a pseud-C&C server instead of the real C&C server.
- Our technology aims to obtain disabling information from various IoT malware, and detect and disable IoT malware with IoT device.

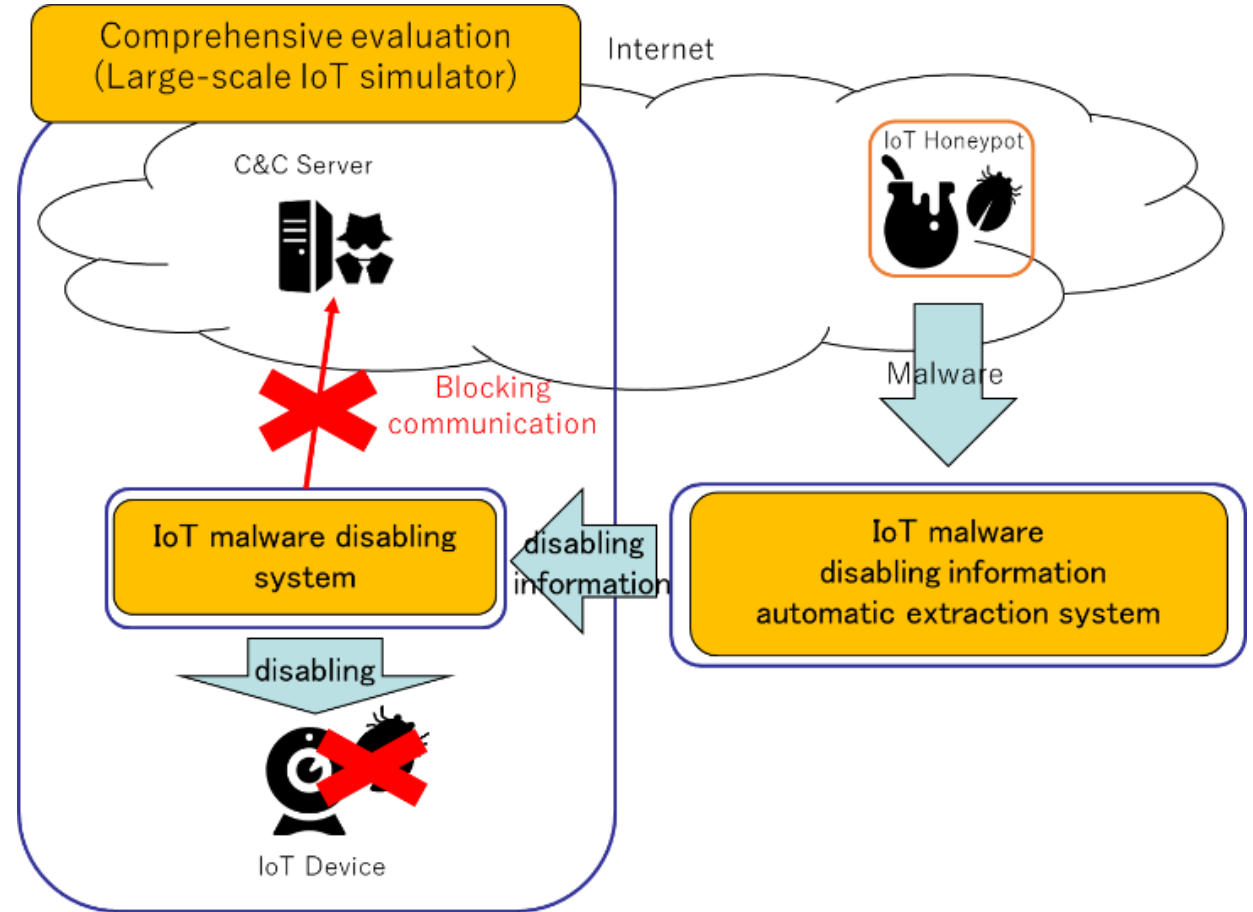


Takeshi Misu, Tatsuaki Momoi, "Proposal of IoT malware removal method using dummy C&C server," 2019 Symposium on Cryptography and Information Security(SCIS 2019), 3E2-2, IEICE, Jan. 2019.

# Overview

Our disabling technology consists of two main systems.  
And we build a simulator for evaluation.

- A) IoT malware disabling-information automatic extraction system.
- B) IoT malware-disabling system
- C) Large-scale IoT simulator

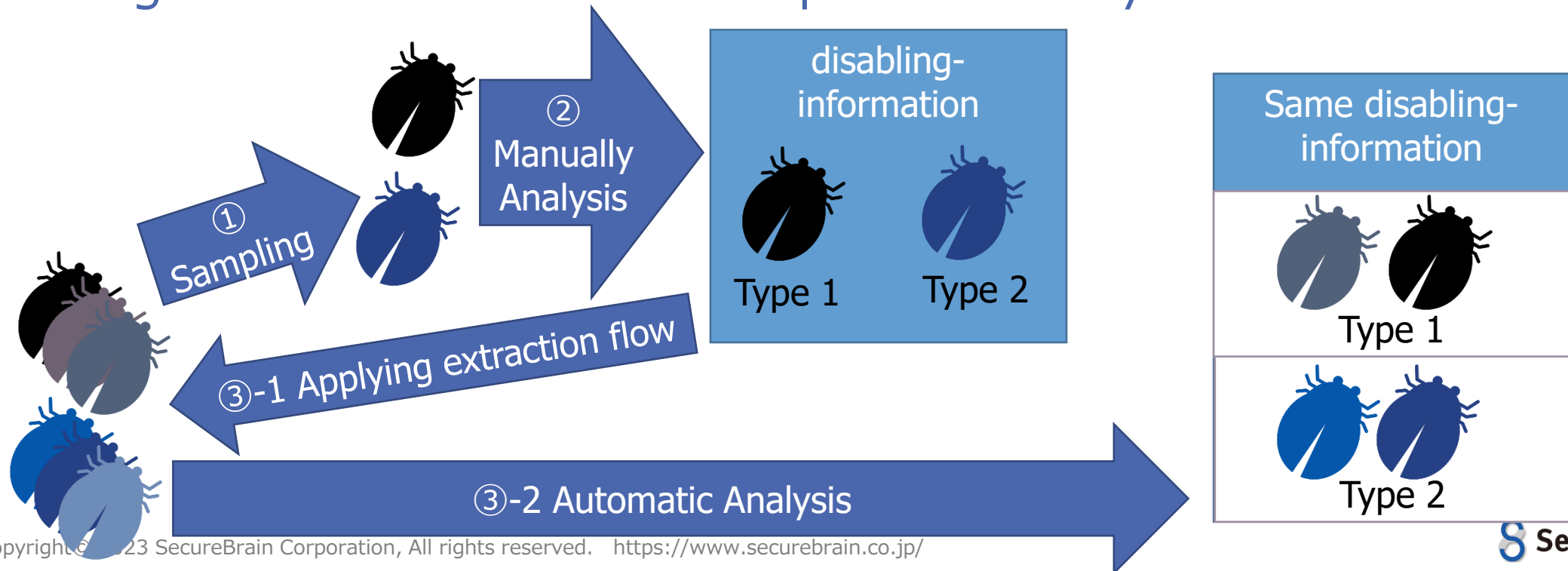




# A) IoT malware disabling-information automatic extraction system

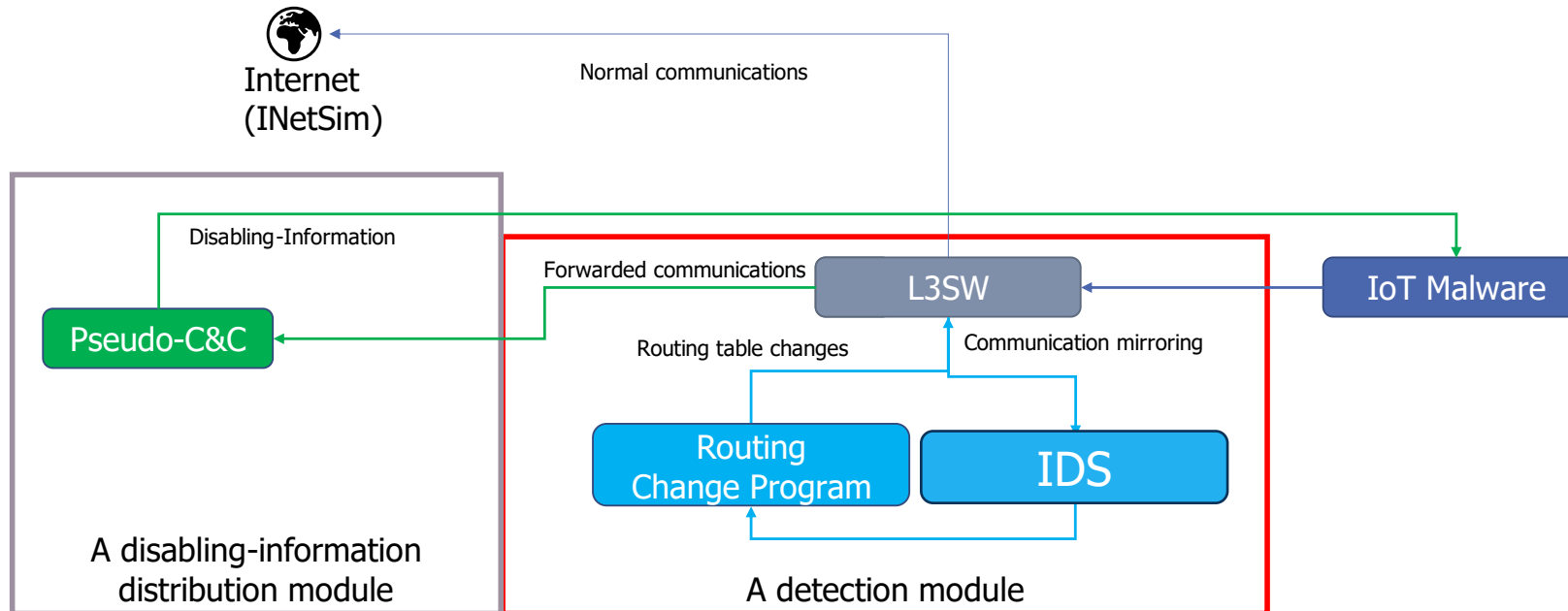
This system uses an automatic extraction method that extracts disabling-information from the IoT malware.

We employ this system because malware with the same name often exhibit different behaviors and require different disabling information, depending on the customization implemented by the attacker.



## B) IoT malware-disabling system

- The detection module
  - The detection module detects the communication to the C&C server from the IoT malware, and forwards it to the disabling-information distribution module
- The disabling-information distribution module
  - The disabling information distribution module transmits the disabling information to the IoT malware.



# Evaluation: Automatic extraction of the disabling information

## Evaluation malware samples

- We evaluated the IoT malware disabling-information automatic extraction system using 4,953 samples.
- The samples were selected from 32,734 IoT malware samples collected by the advanced IoT Honeypot[3][4][5] from June 2021 to March 2022.
- The samples were ARM and MIPS binary that worked on QEMU user mode.

[3] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.

[4] Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Vol. 57, No. 4, 2016.

[5] Seiya Kato, Rui Tanabe, Katsunari Yoshioka, Tsutomu Matsumoto, "Adaptive Observation of Emerging Cyber Attacks targeting Various IoT Devices," IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021.

# Evaluation: Automatic extraction of the disabling information

Extraction results	Samples
Extracted	1,333
Partial	1,137
not Extracted	2,483
Total	4,953

“Extracted” means the system was able to extract the disabling information from the samples.

“Partial” means the system extracted some information from the samples, but it was not the correct disabling information.

“not Extracted” means the system determined that samples don’t have the disabling information.

# Evaluation: IoT malware-disabling

## Evaluation malware samples

We evaluated using 1,333 samples that were able to extract the disabling information.

Extraction results	Samples
Extracted	1,333
Partial	1,137
not Extracted	2,483
Total	4,953

# Evaluation: IoT malware-disabling

Disabling results against only “Extracted” samples

Determination	Mirai	Bashlite	Total
Disabled	775(93.42%)	499(99.01%)	1274(96.00%)
Detected (sinkhole)	48(5.83%)	5(0.99%)	53(3.99%)
Failed	0(0.00%)	0(0.00%)	0(0.00%)
Total	823	504	1327

"Disabled" is successful in detecting and disabling the samples.

"Detected" is successful only in detecting.

"Failed" is a failure of both.

The disabling success ratio against Extracted samples by the system is 96.0%.

\*Excluding 6 samples that didn't work in evaluation process.

# Evaluation: IoT malware-disabling

Evaluation against Partial and not Extracted samples

We considered ways of disabling these samples.

If the malware communication can be detected it can be forwarded to the pseud-C&C server.

Extraction results	Samples
Extracted	1,333
Partial	1,137
not Extracted	2,483
Total	4,953

# Evaluation: IoT malware-disabling

Detecting results against Partial and not Extracted samples

Determination	Result
Detected (sinkhole)	3529(98.93%)
Failed	38(1.07%)
Total	3567

Almost all not extracted the disabling information samples were able to be detected.

The system is able to disrupt the communication from the malware that cannot be disabled.



# Comprehensive Evaluation of the IoT malware disabling system

We build the Large-scale IoT simulator based on ns-3 network simulator.

The sub-simulators for IoT malware activity simulation:

1. Infection spread simulation: Simulates the spread of the IoT malware in a large-scale IoT environment.
2. DDoS attack simulation: Simulates DDoS traffic from infected IoT devices targeted at a specific server.

The IoT malware disabling simulator: Simulates the behavior of the IoT malware disabling system.

# Evaluation Conditions

Our developed large-scale IoT simulator was used to evaluate the performance of the mentioned IoT malware-disabling technology in a large-scale environment with large number of IoT devices.

The experimental conditions can be seen in the table.

Note that because the background traffic is using TCP, the intended network traffic may not be achieved because of congestion control algorithms and queuing delays.

Simulation time	10 s
Attack duration	5 s
Attack type	UDP
Send data(Excluding headers)	474 bytes
Attack packet interval	0.000399
Number of nodes	1000
Number of infected nodes	1000
Number of nodes per components	25
Bottleneck bandwidth	2.5 Gbps
Backend traffic usage	50%, 70%
Application rate of the disabling method	0, 25, 50, 60, 70, 80, 90, 100

# Evaluation result for 50% backend traffic utilization

x-axis:

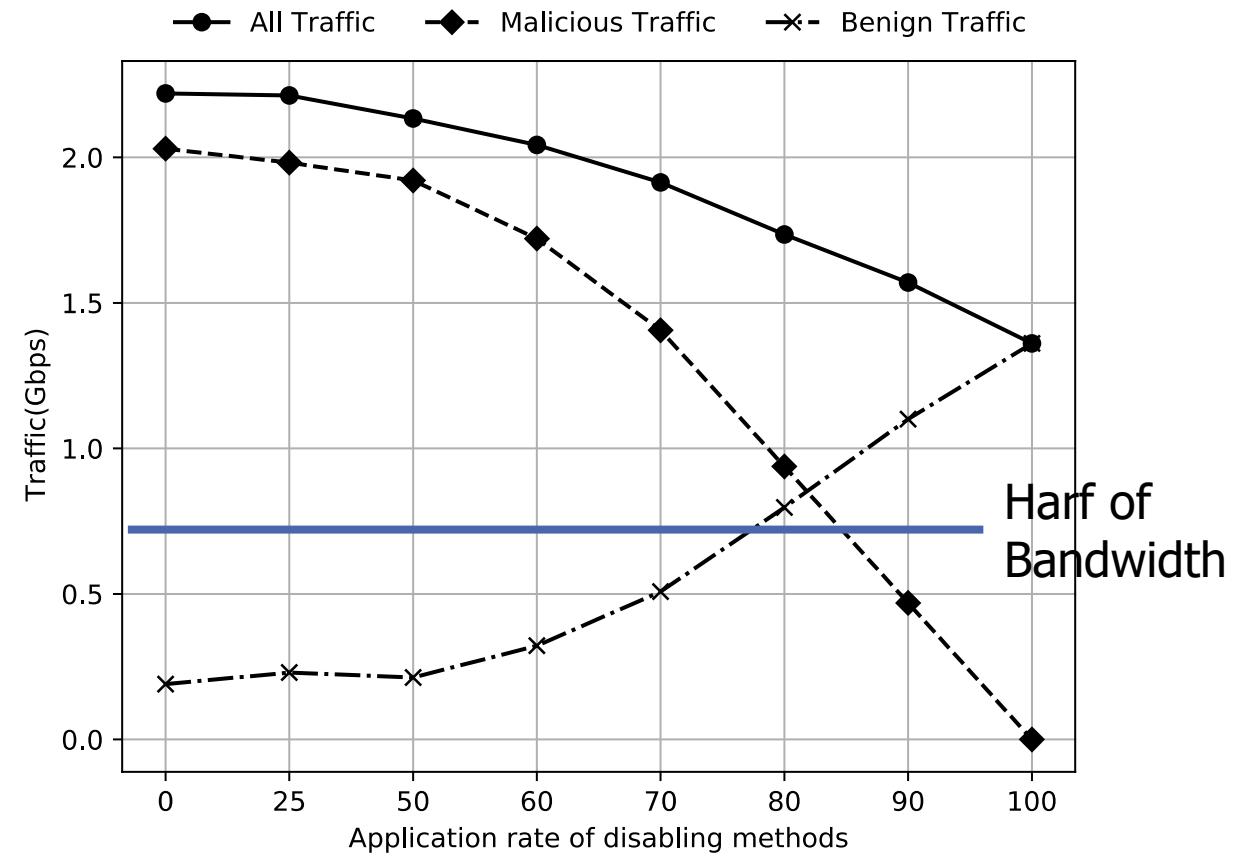
The percentage of IoT malware disabled networks.

y-axis:

The amount of traffic flowing into the network.

"All Traffic" means the sum of background traffic and DDoS traffic.

Simulation results indicate that applying the method to 80% of the networks is necessary to achieve a bandwidth availability of approximately 50% of the background traffic.



# Conclusion

- The IoT malware disabling information automatic extraction system is able to extract the disabling information from a certain number of IoT malware.
- The IoT malware disabling system is capable of disabling the IoT malware using the disabling information of the extraction results.
- Evaluation of our proposed IoT malware-disabling technology using the large-scale IoT simulator showed that it's necessary to disable 80% of the IoT malware on the network in order to mitigate the effects of DDoS attacks on the network.

# Future work

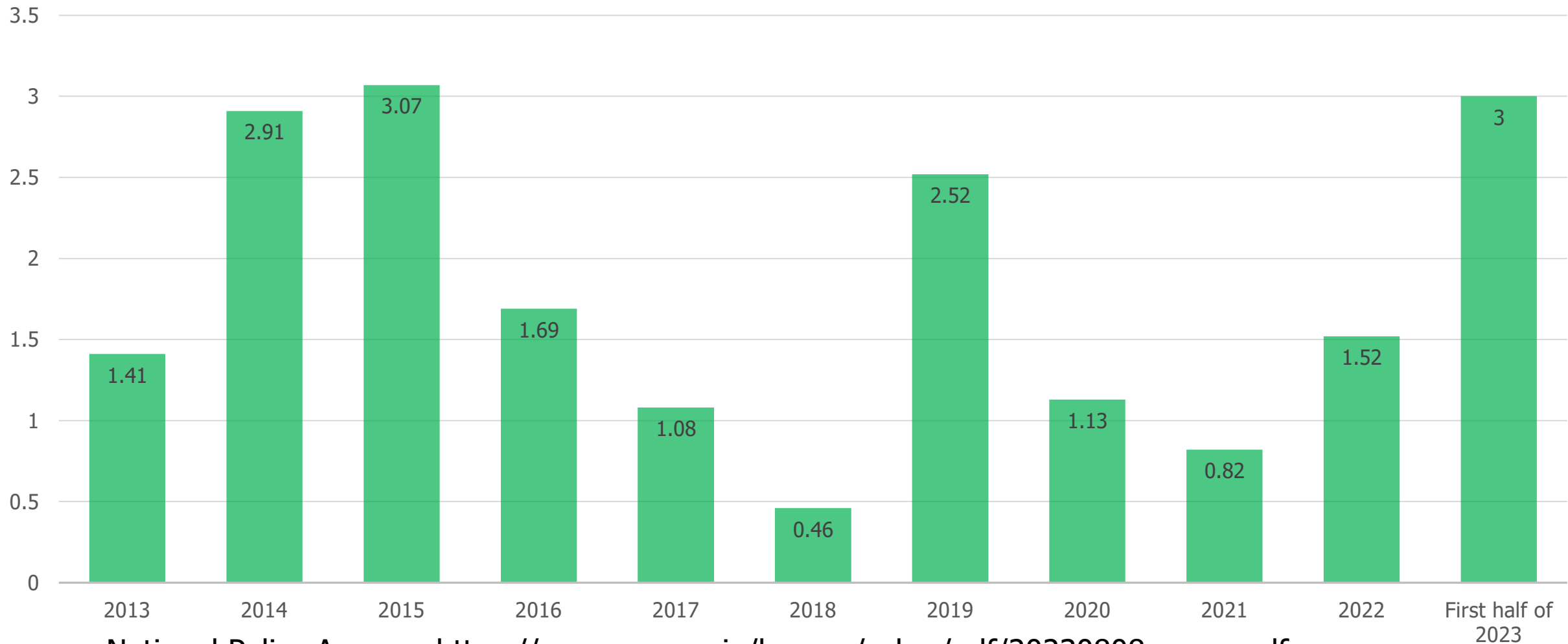
- We aim to apply this technology to the real world and promote its dissemination in society.
- Therefore, we need to:
  - It should be continued accuracy improvement and expansion of target malware about these systems.
  - It is necessary to evaluate by simulating more accurately reflect a more realistic network setup and bandwidth.



# For Reduction of Phishing Scam

# Illegal remittance through Internet banking due to phishing in Japan

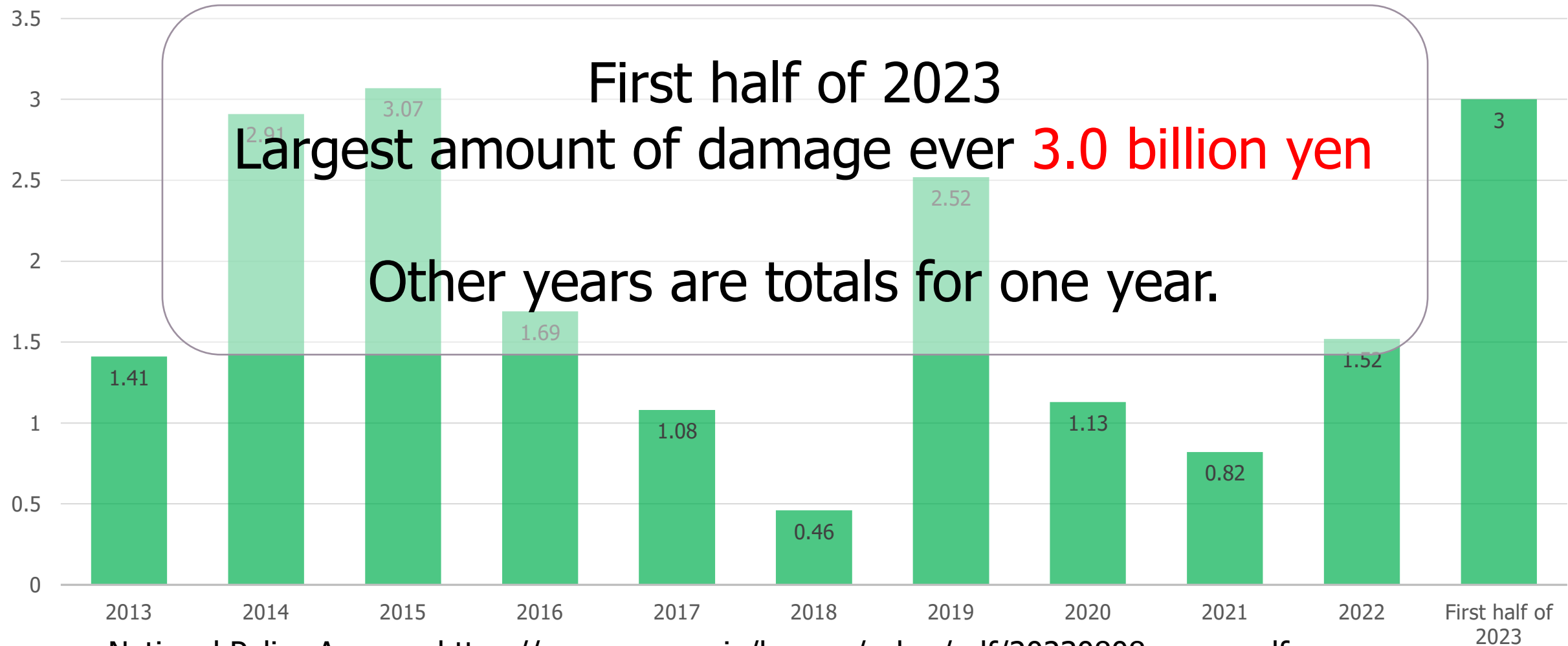
Damage amount (Billion yen)



National Police Agency: [https://www.npa.go.jp/bureau/cyber/pdf/20230808\\_press.pdf](https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf)

# Illegal remittance through Internet banking due to phishing in Japan

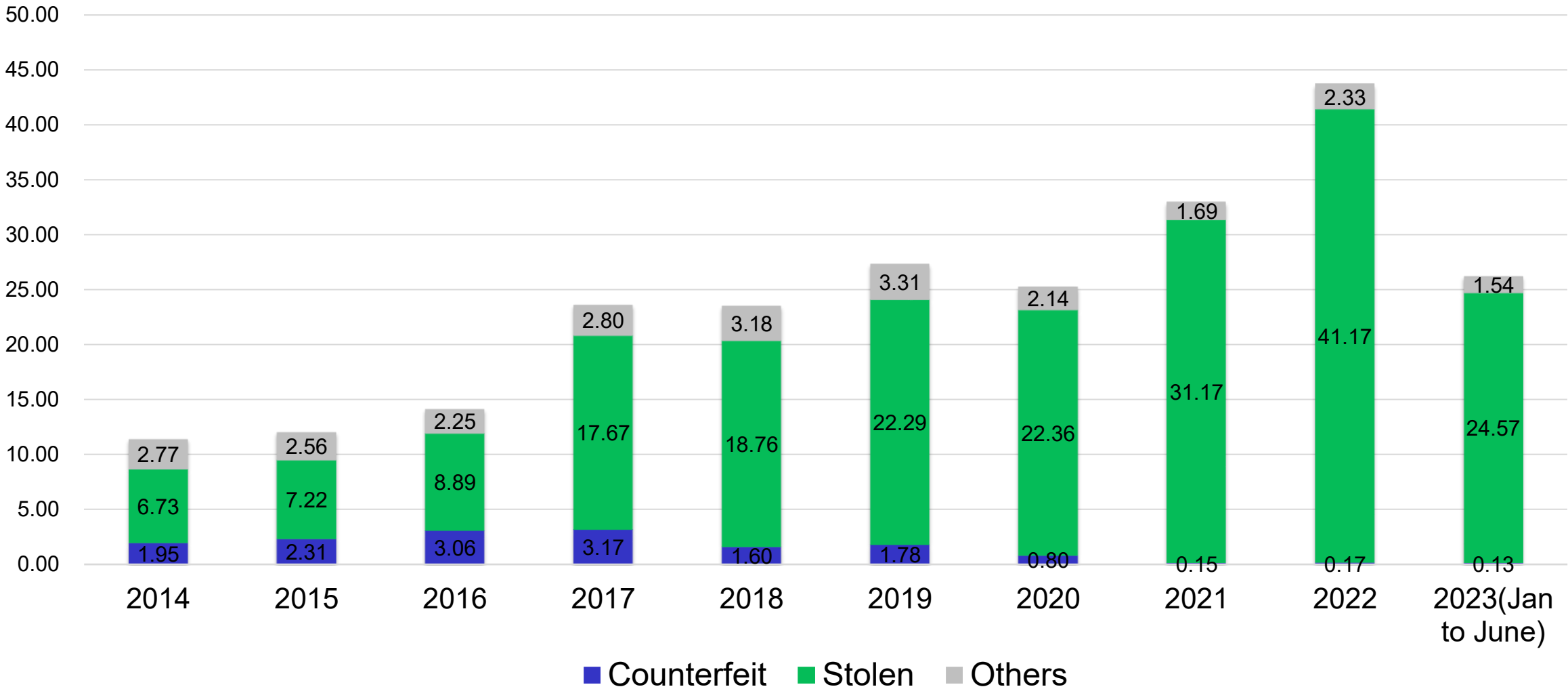
Damage amount (Billion yen)



National Police Agency: [https://www.npa.go.jp/bureau/cyber/pdf/20230808\\_press.pdf](https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf)

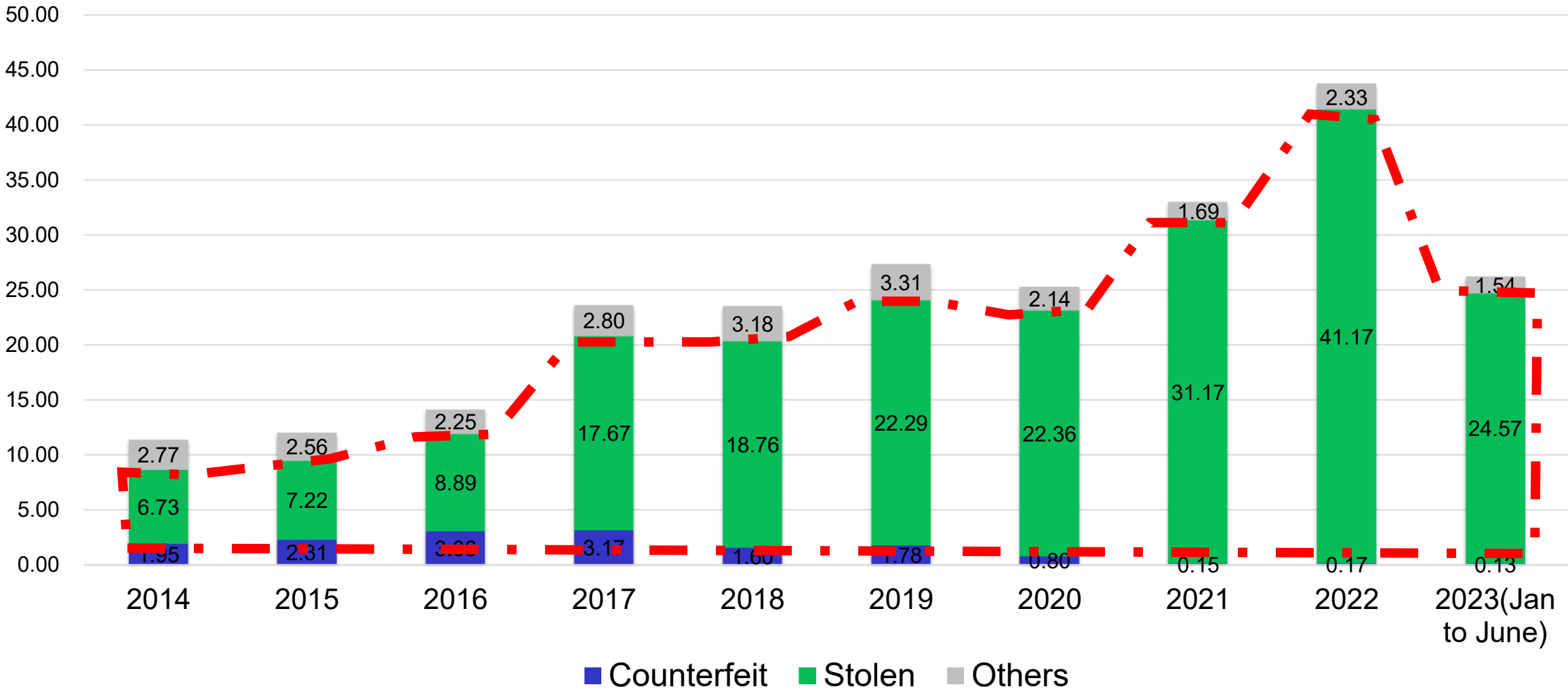


# Amount of damage caused by fraudulent credit card use in Japan



[https://www.j-credit.or.jp/information/statistics/download/toukei\\_03\\_g.pdf](https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf)

# Amount of damage caused by fraudulent credit card use in Japan



[https://www.j-credit.or.jp/information/statistics/download/toukei\\_03\\_g.pdf](https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf)

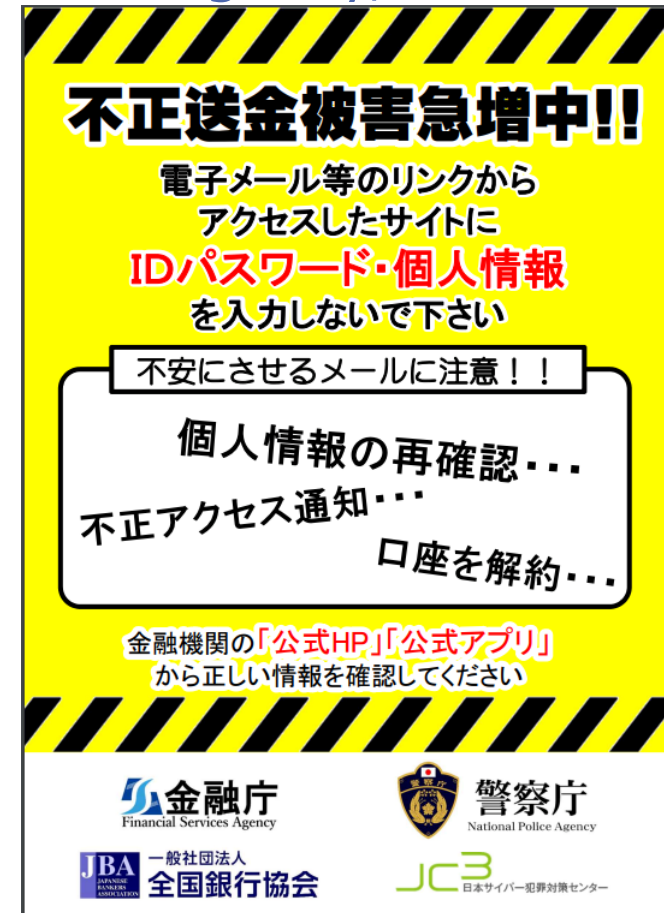
# The current state of phishing in Japan

Phishing amount of damage has been increasing in Japan.

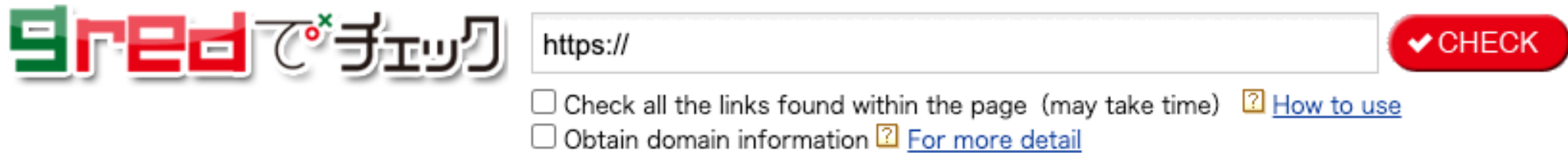
In particular, the damage caused by phishing attacks targeting Internet banking users continues to reach record levels.

Japanese administrative agencies and other organizations are promoting awareness and recommending countermeasures.

Alert poster from Financial Services Agency, National Police Agency, and others.



# Data collection



The screenshot shows the 'gred de check' website interface. On the left is the logo 'gred で チェック' (gred de check). To its right is a text input field containing 'https://'. Further right is a red button with a white checkmark and the text 'CHECK'. Below the input field are two checkboxes: the first is 'Check all the links found within the page (may take time)' with a link to 'How to use'; the second is 'Obtain domain information' with a link to 'For more detail'.

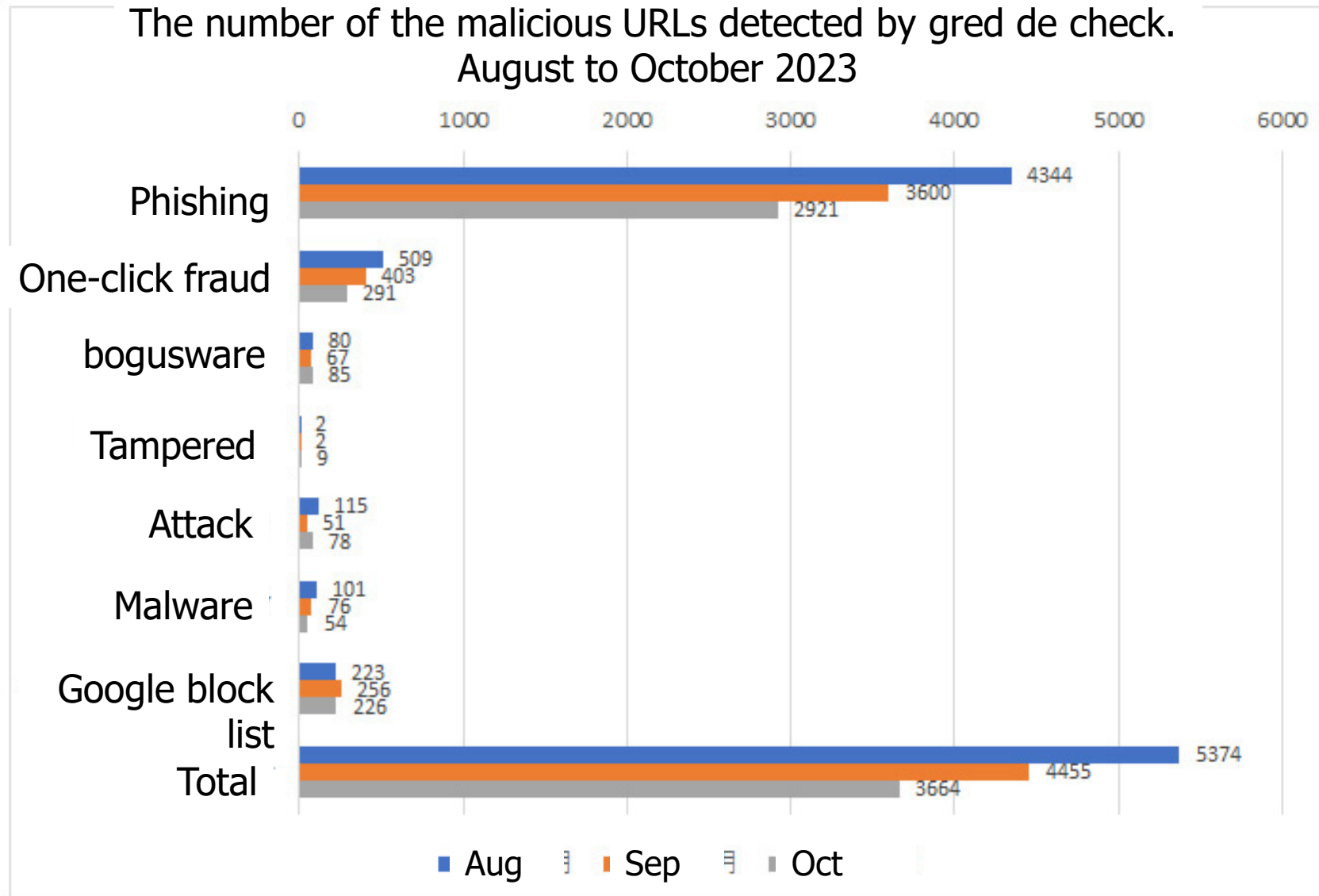


<https://check.gred.jp/>

We are providing a free website checker that is “gred de check”. “gred de check” possesses a heuristic engine that checks the contents of the website.

Users can check whether the website is malicious or not only by inputting the URL.

# Data collection



# Cooperation

- Council of Anti-Phishing Japan

Promotion of countermeasures focusing on activities such as collecting and providing information and alerting the public about phishing.

SecureBrain is a members of the Council of Anti-Phishing Japan.

## Our activities

- Member of the Academic Research Working Group.
  - Member of the Phishing-site Response Automation Task Force
- 
- Metropolitan Police Department

MPD and SecureBrain have concluded a mutual cooperation agreement to prevent cybercrime since 2014.

# Research

- Analysis and Consideration of Detection Methods to Prevent Fraudulent Access by Utilizing Attribute Information and the Access Log History[6]
  - We analyzed the attacker's device attribute information and the differences in the environments of legitimate users and fraudsters using the server-side access log history of actual services.
  - We also propose an effective detection method using real-world data.

[6] Michio Kunimoto, Takao Okubo, Analysis and Consideration of Detection Methods to Prevent Fraudulent Access by Utilizing Attribute Information and the Access Log History, Journal of Information Processing, vol.31, pp. 602-608, 2023

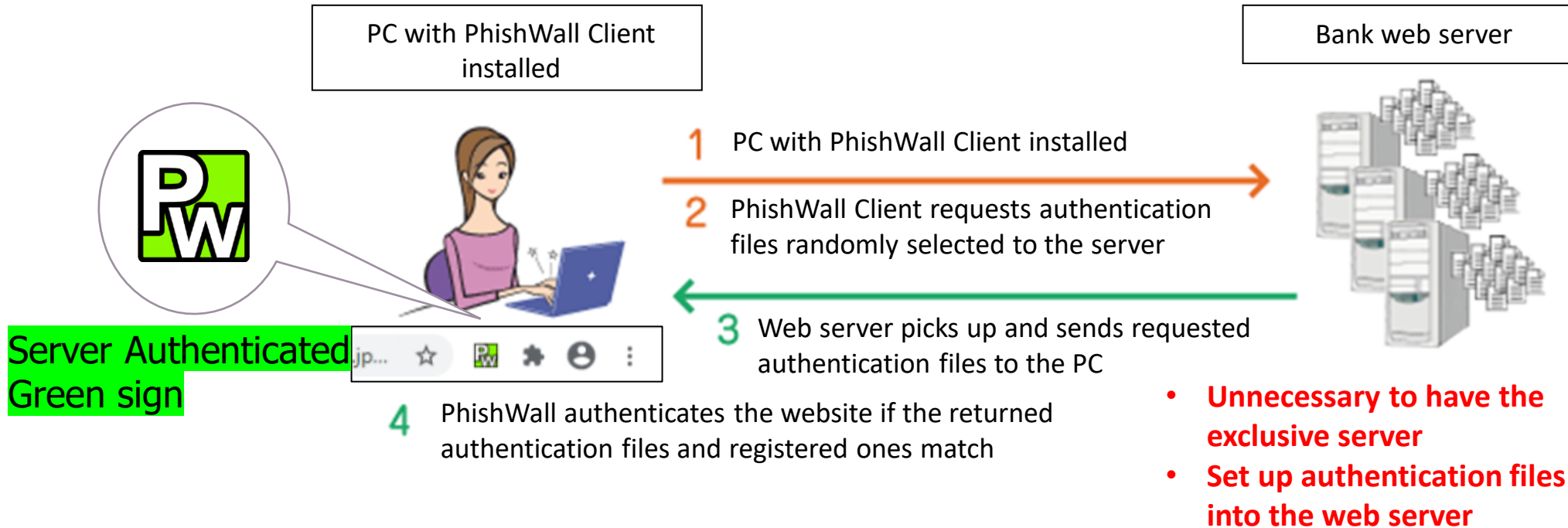
# Solutions

Solution	Function
PhishWall Premium	<u>Anti-Phishing</u> Detection of MITB(Man-in-the-Browser) attacks
PhishWall Clientless	Detection of MITB attacks
SecureBrain Scam Radar BD	<u>Detection of spoofed access</u>



# PhishWall Premium Anti-Phishing

## PhishWall Authentication

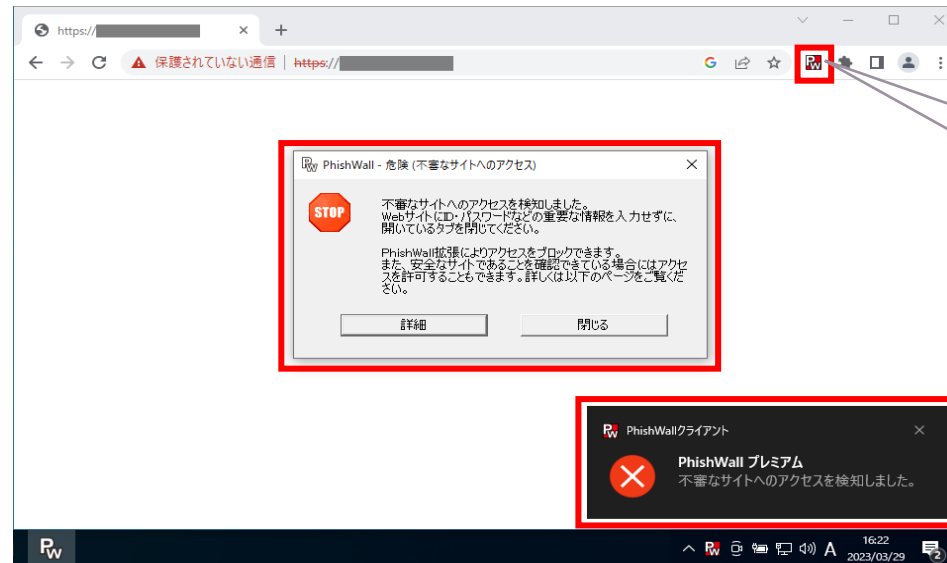


Users can check the legitimate sites by PhishWall Authentication **Green sign.**

# PhishWall Premium Anti-Phishing

## Detection of access to fraudulent site

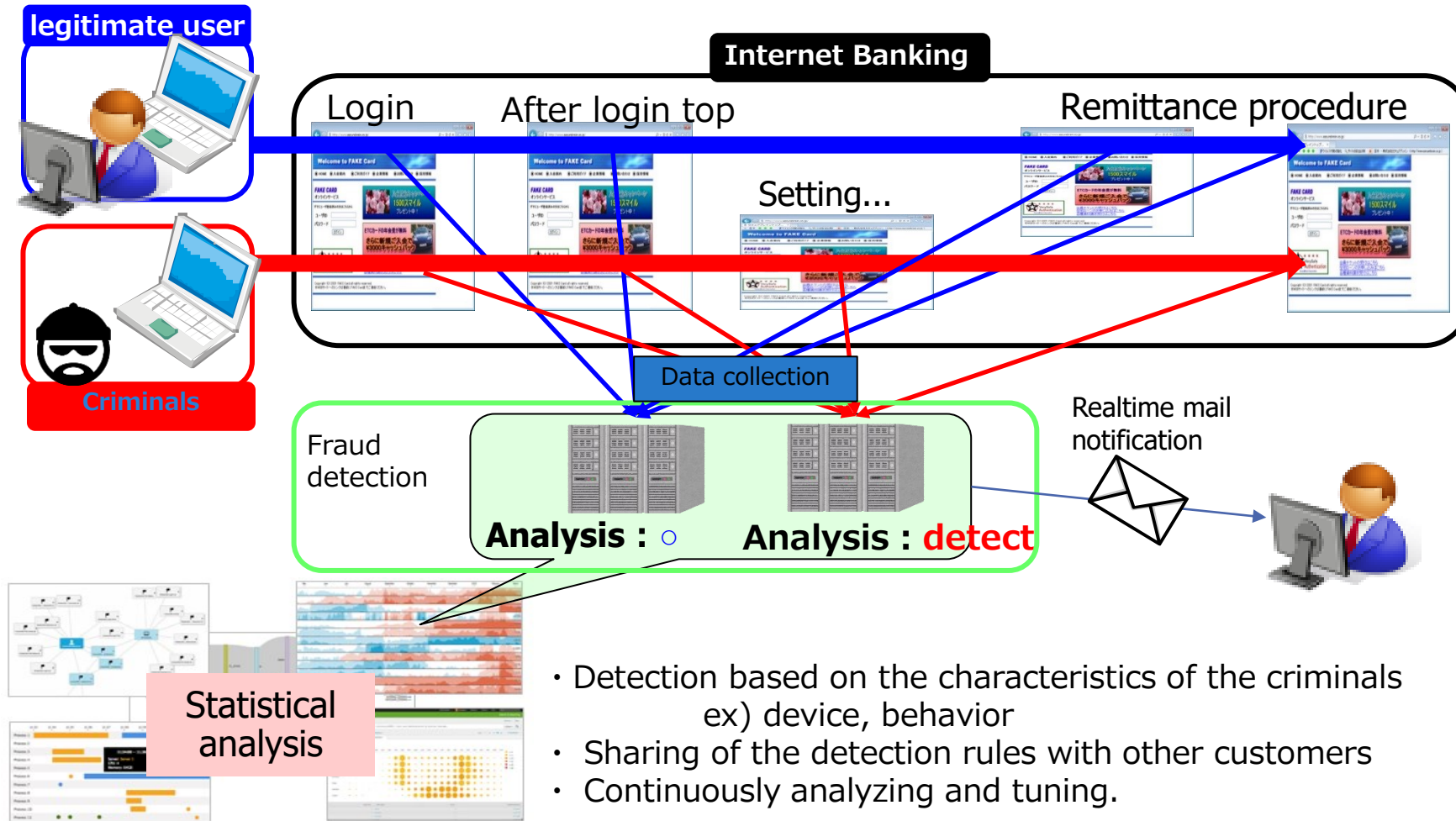
- PhishWall displays a warning message when it detects access to a fraudulent site via the web browser.



Detected access to a fraudulent site

# SecureBrain Scam Radar BD

## Detection of spoofed access



# User benefits of Scam Radar BD

Monitoring agency on behalf of customers with fraud detection features and its continuous tuning

- a. Detect based on comprehensive profile analysis of the attacker's terminal by browser/device fingerprint technology etc.
- b. SecureBrain tunes Scam Radar BD continuously, so customers don't have to tune by themselves, so operation cost can be reduced and they can start to utilize it without tuning experience.
- c. Not only suspicious indicators on IP addresses, languages and user agents as well as fraudulent behaviors are analyzed.
- d. Tuned by SecureBrain and not black-boxed, so Scam Radar detects suspicious access with explaining reasons which is useful when inquiring end users or reporting transactions to authorities.

# Thank you for your attention!



Collaboration or work together  
is crucial in the fight against cybercrime!



# ネット犯罪からすべての 人を守る

Our Knowledge, Your Security.