RITSUMEIKAN UNIVERSITY

Exploration of Cybersecurity Posture: Analysis of Global IP Addresses and External Services in Small and Medium-sized Enterprises

Keisuke Tanaka
Ritsumeikan University
TrendMicro Inc

Yuuki Kimura
Ritsumeikan University

Soma Sugahara
Ritsumeikan University

Tetsutaro Uehara
Ritsumeikan University

Futurize.
きみの意志が、未来。

Outline

- INTRODUCTION
- SUMMARY OF STUDY
- RELATED WORK
- RESEARCH METHOD
- RESULTS
- POSSIBLE IMPROVEMENTS
- CONCLUSION

Outline

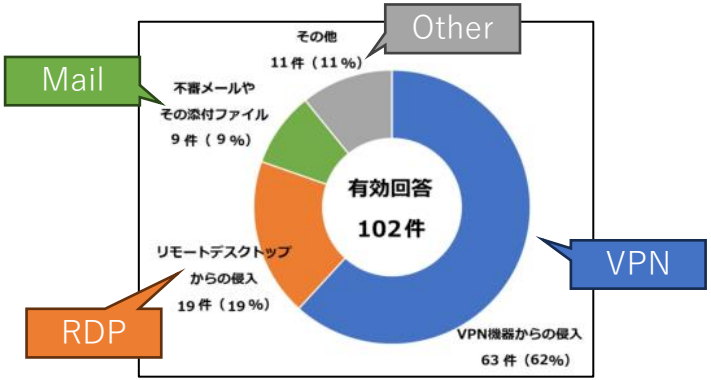
- **INTRODUCTION**
- SUMMARY OF STUDY
- RELATED WORK
- RESEARCH METHOD
- RESULTS
- POSSIBLE IMPROVEMENTS
- CONCLUSION

INTRODUCTION

- Cyber attacks are active in the corporate environment
- It is reported that direct intrusion into an external service, including Virtual Private Network (VPN) devices and server remote desktops(RDP), accounts for 81% of the entry points for ransomware attacks

> ***Ransomware*** *is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.*

Trendmicro: Ransomware Definition
https://www.trendmicro.com/vinfo/ph/security/definition/Ransomware



National Police Agency: Threats in Cyberspace
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

Outline

- INTRODUCTION
- **SUMMARY OF STUDY**
- RELATED WORK
- RESEARCH METHOD
- RESULTS
- POSSIBLE IMPROVEMENTS
- CONCLUSION

RITSUMEIKAN UNIVERSITY

SUMMARY OF STUDY

Objective

- To understand the current state of risks associated with Global IP addresses and external services in SMEs.

Research Question

- To what extent do external services with a real risk of cyberattacks actually exist?

SUMMARY OF STUDY

Target

- SMEs
- Information security personnel

Contribution Details

- The research results and methodology can serve as a reminder and reference for improving a company’s own security measures.

RITSUMEIKAN UNIVERSITY

Outline

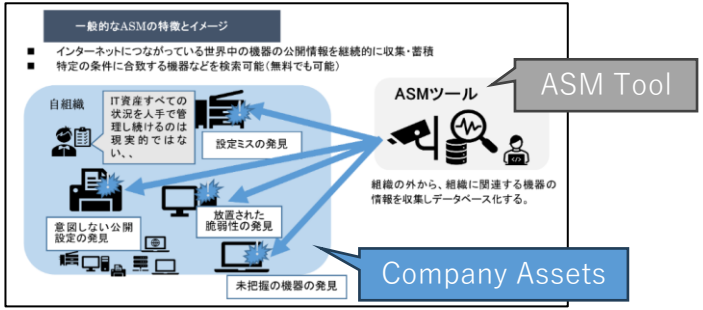
- INTRODUCTION
- SUMMARY OF STUDY
- **RELATED WORK**
- RESEARCH METHOD
- RESULTS
- POSSIBLE IMPROVEMENTS
- CONCLUSION

RELATED WORK

- Existing guidance about Attack Surface Management
  - Recently, a concept and service known as Attack Surface Management (ASM) has gained traction as a method for visualizing the IT assets and risks of SMEs.
    - Release guidance from The Ministry of Economy, Trade, and Industry of Japan
  - However, this guidance provides only an overview and examples of the ASM concept and its applications, without mentioning specific ASM tools, services, selection methods, or usage instructions.

Attack Surface Management (ASM) is the process of continuously identifying, monitoring and managing all internal and external internet-connected assets for potential attack vectors and exposures.

What is attack surface management?
https://www.paloaltonetworks.com/cyberpedia/what-is-attack-surface-management



Guidance of ASM (Attack Surface Management)
https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

RELATED WORK

- Existing of ASM Service
  - There are many ASM services by security companies.
  - But it is expensive and excessive for a SMEs to conduct first surveys.
  - A wide range of survey items seems too much for SMEs.

- Out focus…
  - We focus solely on Global IP addresses and their external services to facilitate SMEs' engagement with ASM.
  - We will then verify whether security risks can be visualized through this study, making it more feasible for SMEs to conduct their initial security risk assessments.

Outline

- INTRODUCTION
- SUMMARY OF STUDY
- RELATED WORK
- **RESEARCH METHOD**
- RESULTS
- POSSIBLE IMPROVEMENTS
- CONCLUSION

Research Method - Recruitment

- Jointly with the Osaka Chamber of Commerce and Industry, we solicited companies that wish to participate in the security risk survey.
- 83 SMEs participated to our survey.

OVERVIEW OF PARTICIPATING COMPANY RECRUITMENT

Item	Content
Implementation Period	May 23, 2023 - July 31, 2023
Recruitment Method	Web Page
Number of Target Companies	83 companies
Number of Target IP Addresses	156 addresses

Research Method - Recruitment

- The distribution of participating companies is shown in the table below.

NUMBER OF EMPLOYEES

Number of Employees	Count	Percentage
0～5	12	14%
6～10	6	7%
11～20	21	25%
21～50	15	18%
51～100	13	16%
101～300	12	14%
301人～	4	5%

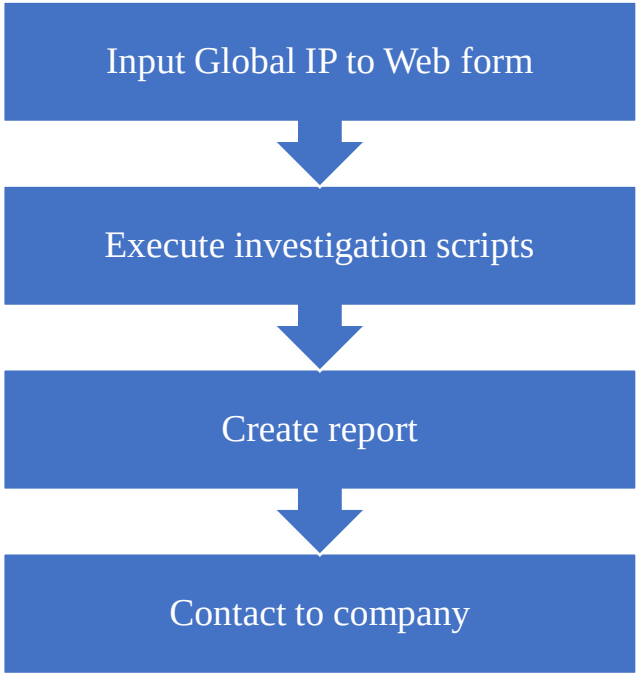
PRESENCE OF INFORMATION SYSTEMS PERSONNEL

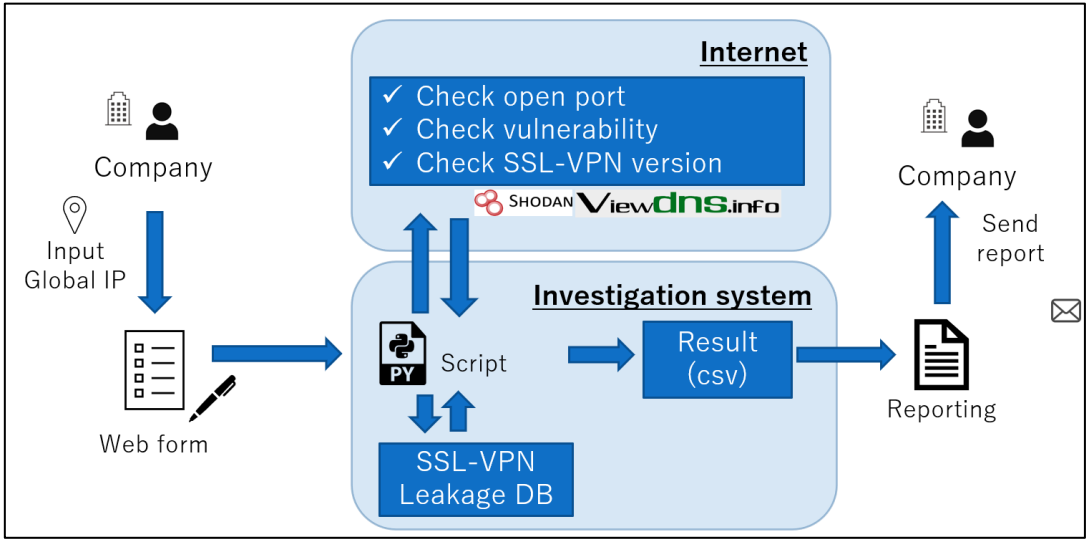
Information Systems Personnel	Count	Percentage
None	25	30%
Exists	58	70%

INDUSTRY CLASSIFICATION (MAJOR CATEGORIES)

Industry	Count	Percentage
Service Industry	25	30%
Manufacturing Industry	18	22%
Wholesale and Retail Trade	15	18%
Academic Research, Professional and Technical Services Industry	7	8%
Information and Communication Industry	5	6%
Unclassified Industries	4	5%
Medical and Welfare Industry	3	4%
Accommodation and Food Services Industry	2	2%
Construction Industry	1	1%
Electricity, Gas, Heat Supply, and Water Supply Industry	1	1%
Financial and Insurance Industry	1	1%
Real Estate and Goods Leasing Industry	1	1%

Research Method – Investigation Methodology





Overview of Investigation

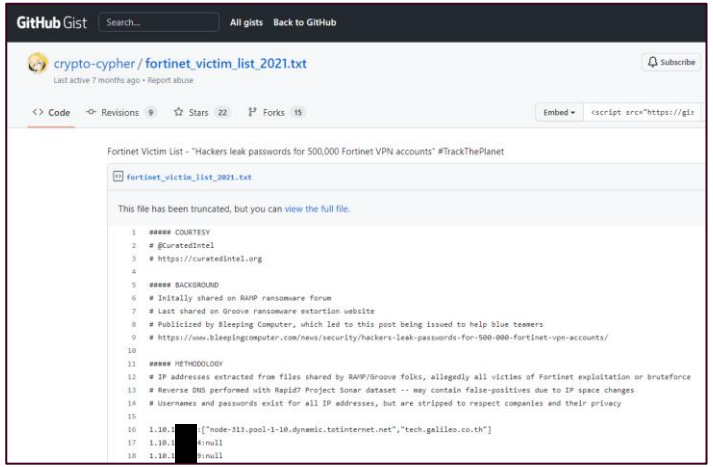
Research Method – Investigation Items

Investigation item to each global IP are below five items.

1. Open Ports with Risks
2. Vulnerabilities in Open Ports
3. SSL-VPN with Leaked Authentication Information
4. Outdated Versions of SSL-VPN (Fortigate)
5. Unnecessary Exposure of External Access

Reference : Match with leak SSL-VPN information

- Fortigate IP and ID/Password leaks in the past
- We matched it with the leaked IP addresses (about 80,000) that we were able to obtain



Outline

- INTRODUCTION
- SUMMARY OF STUDY
- RELATED WORK
- RESEARCH METHOD
- **RESULTS**
- POSSIBLE IMPROVEMENTS
- CONCLUSION

Result

- 11 out of 83 companies (13%) have global IP addresses with security risk
- Results of each survey item are below.
  1. Opening of Ports at Risk: 5 Companies
  2. Vulnerable to open ports: 5 companies
  3. SSL-VPN with leaked credentials: 0 companies
  4. SSL-VPN (Fortigate) is not up to date: 2 companies
  5. Exposure of risky pages that do not need to be disclosed externally: 3 companies

Results (Survey items × companies)

Company	Survey Items				
	1	2	3	4	5
A				✓	
B				✓	
C		✓			✓
D		✓			
E		✓			
F	✓	✓			✓
G		✓			
H	✓				✓
I	✓				
J	✓				
K	✓				

Results – Detailed (Survey item 1.2)

- 5 out of 83 companies (6%) confirmed that they had opened risky ports.
- Remote desktop port (3389/TCP) ,file sharing port (445/TCP) was not confirmed to be open.
- 5 out of 83 companies (6%) were found vulnerabilities.

Result of port checking

	3389	445	22	23
Port Opening	0	0	3	2
Port blockage	83	83	80	81
Percentage of opening	0%	0%	3.6%	2.4%

Number of vulnerabilities

ID*	Number of vulnerabilities
O-020	50
O-028	167
O-084	1
O-126	51
O-135	47

*Assign a unique identifier to the global IP address to be investigated

Results – Detailed (Survey Items 3 and 4)

- Nothing was found to match the list of "IP addresses whose credentials have been leaked in the past“.
- Of the 12 out of 83 (14%) Fortigate IP addresses, 2 (16%) were more than one year old and 6 (50%) were more than six months old after update of firmware.

Fortigate：Days since last update of firmware

Elapsed days	Count	Percentage
Over 1 years (365-)	2	16%
Over half of year (183-364)	6	50%
Under half of year (-183)	4	33%

Fortigate：Version Distribution

ID	Ver	Released	Elapsed Days
O-015	6.2.12	2022/11/3	270
O-024	6.0.16	2022/12/15	228
O-031	6.4.8	2021/11/18	620
O-043	6.2.13	2023/2/23	158
O-052	6.2.13	2023/2/23	158
O-059	7.0.10	2023/2/23	158
O-068	6.4.8	2021/11/18	620
O-073	6.0.16	2022/12/15	228
O-075*	7.0.11	2023/3/16	137
O-081*	7.0.11	2023/3/16	137
O-122	6.4.11	2022/11/1	272
O-133	7.0.9	2022/11/22	251
O-141	7.0.9	2022/11/22	251

Results – Detailed (Survey Item 5)

- The following three (3.6%) web service pages that are considered unnecessary and risky to be published externally were confirmed

Trac Lightning

Kibana

Cybozu office management page

Results – Additional Investigation

- Conducted additional research to see if simple ID and password authentication is possible.
- Only for companies that have been in contact and have obtained permission.
- Successfully logged in on 1 web page

Additional Findings

Scope of the Survey	Number of Implementations	Implementation results
SSH	3	No problem
Telnet	1	No problem
Web Page	2	One has problem

ID List

root
admin
administrator

Password List

(Blank)	Password1
admin	password1
password	pass1
123456	1234
123456789	(Company name)
1qaz2wsx	(Company name)+1
p@ssw0rd	(Company name)+123
P@ssw0rd	administrator
root	

Results – Feedback from company

- We also conducted a feedback survey about our security assessment and obtained responses from 44% companies.
- 97% said the investigation was either "very useful" or "useful“
- 50% of companies who obtained a report have implemented security measures on the basis of the report.

Result - Research Question

Is it possible to create a mechanism to easily investigate global IP addresses?

- Create system for investigating five survey items
- Two of the five survey items, as well as report creation and corporate communication, are currently manual (not automated) and need to be improved.

How many global IP addresses are at risk of being compromised?

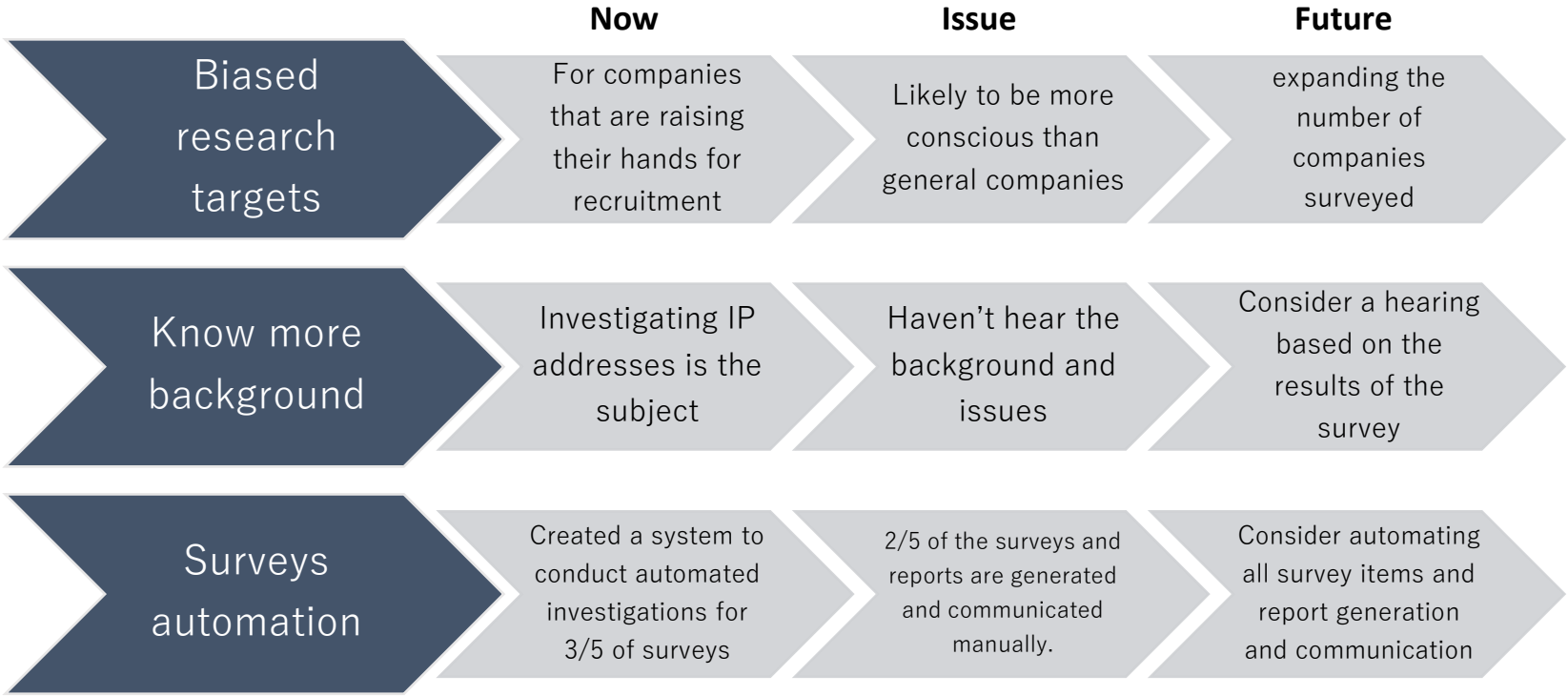
- 11 out of 83 companies (13%) identified IP addresses with security risks
- No risk directly linked to a ransomware attack breach was identified

Outline

- INTRODUCTION
- SUMMARY OF STUDY
- RELATED WORK
- RESEARCH METHOD
- RESULTS
- **POSSIBLE IMPROVEMENTS**
- CONCLUSION

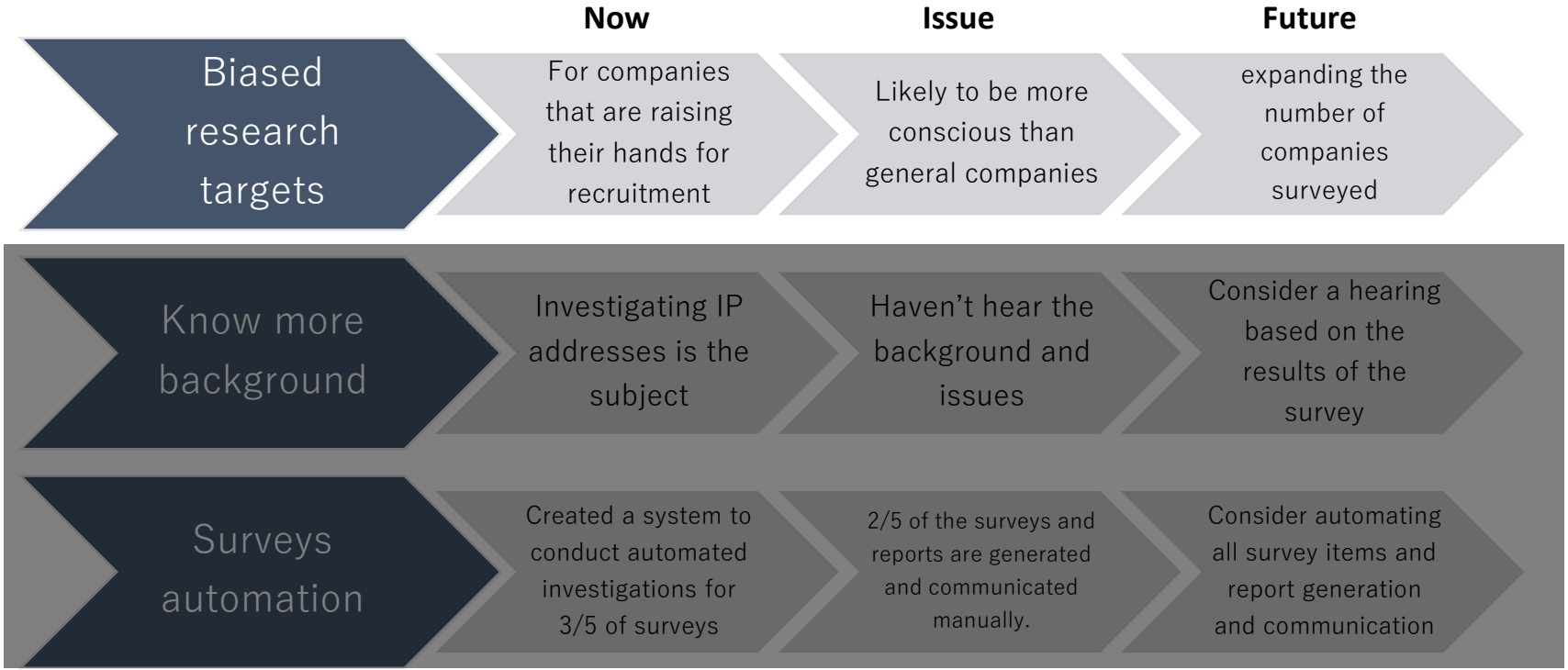
RITSUMEIKAN UNIVERSITY

POSSIBLE IMPROVEMENTS



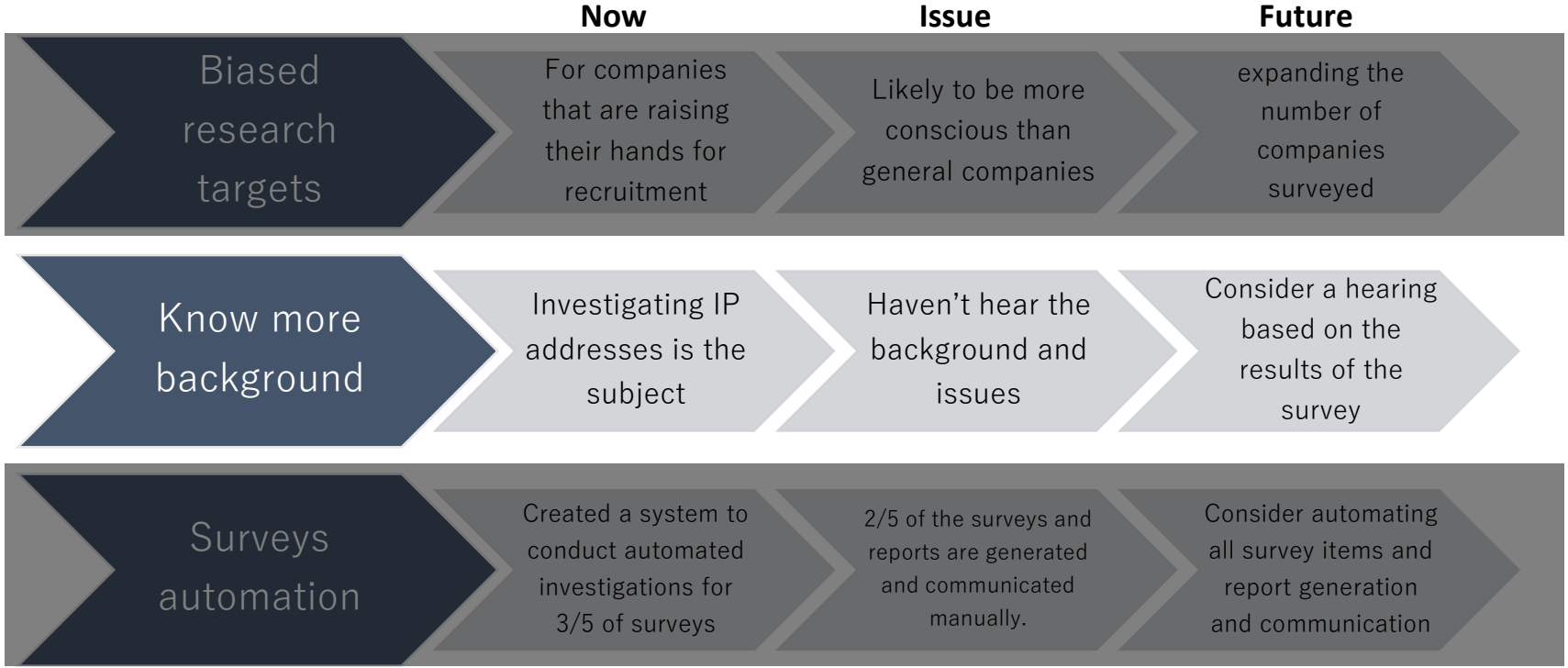
RITSUMEIKAN UNIVERSITY

POSSIBLE IMPROVEMENTS



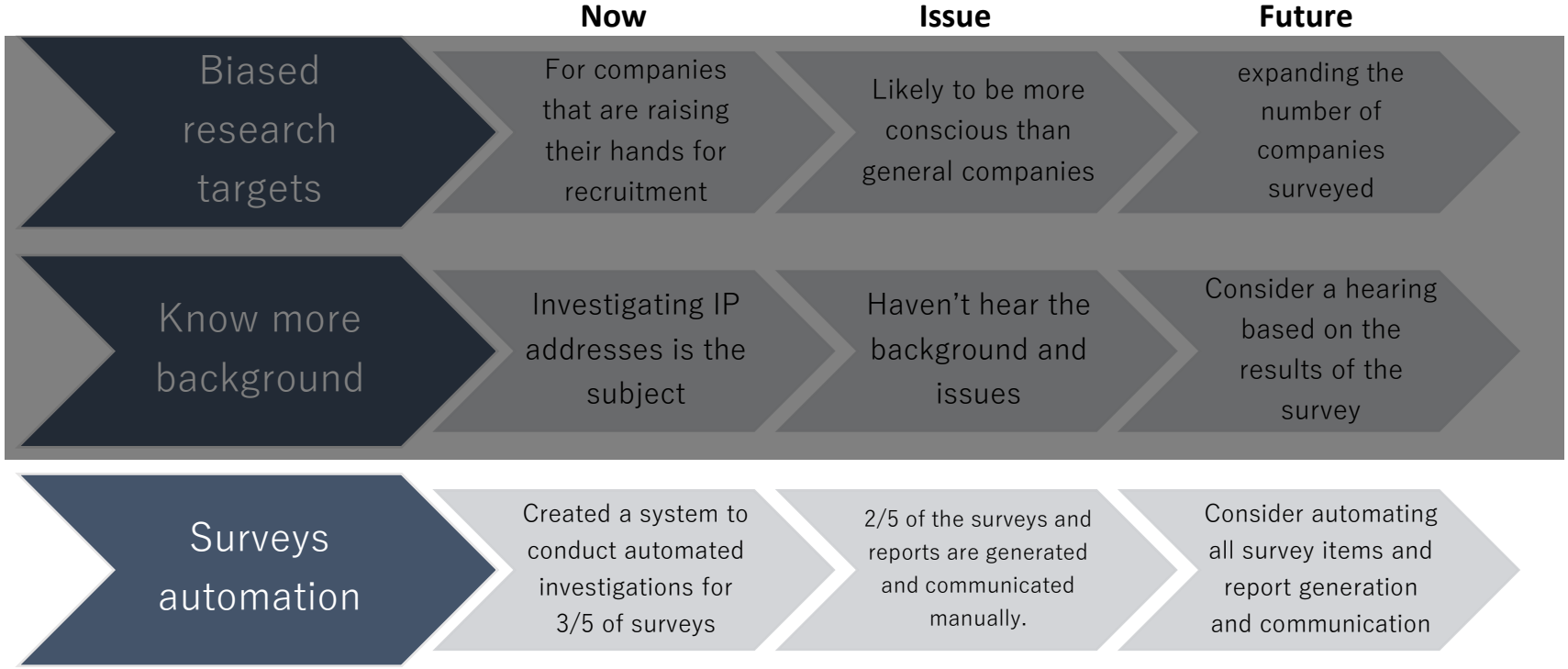
RITSUMEIKAN UNIVERSITY

POSSIBLE IMPROVEMENTS



RITSUMEIKAN UNIVERSITY

POSSIBLE IMPROVEMENTS



Outline

- INTRODUCTION
- SUMMARY OF STUDY
- RELATED WORK
- RESEARCH METHOD
- RESULTS
- POSSIBLE IMPROVEMENTS
- **CONCLUSION**

CONCLUSION

- Methods
  - Investigate security risk of 83 company’s 156 Global IP address.
  - Check five items related recent cyber attack for each Global IP address.
- Results
  - 13% of companies were found security risks, but no risk was found directly related to ransomware attacks.
  - We created semi-automated system to easily check security risk.
  - 97% of companies said the investigation was either "very useful" or "useful“
  - 50% of companies have implemented security measures on the basis of the report.
- Future Tasks
  - Improvements such as better recruitment methods and further automation.
  - Make this research method more widely available, like creating a web service.
  - We should consider interviewing people at selected companies to gain more background and insight.

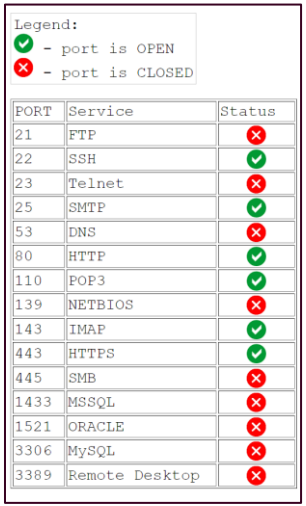
Appendix

Research Method – Investigation Methodology

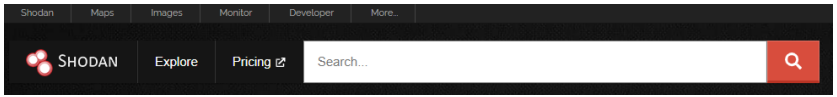
- Utilize the API of an external service (available free of charge)

Check port with ViewDNS

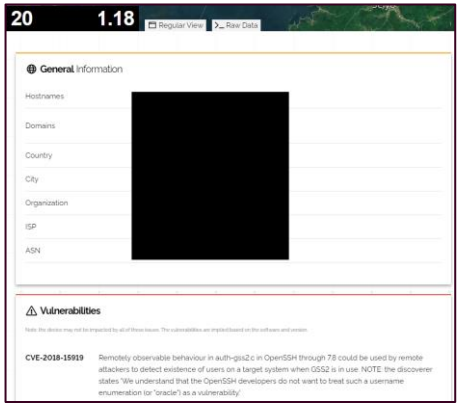
https://viewdns.info/



Check vulnerability by Shodan



https://www.shodan.io/



Research Method – Investigation Methodology

No	IP
O-146	1[redacted]224
O-147	2[redacted]25
O-148	1[redacted]134
O-149	1[redacted]46
O-150	1[redacted]87
O-151	1[redacted]02

SHODAN ViewDNS.info

API

No	IP	3389	445	443	10443	8443	Other Ports	CVEs	Leak
O-146	1[redacted]24	False	False	False	False	False		NaN	False
O-147	2[redacted]25	False	False	True	False	False	4433、541	False	False
O-148	1[redacted]34	False	False	False	False	False		NaN	False
O-149	1[redacted]46	False	False	False	False	False		NaN	False
O-150	1[redacted]87	False	False	False	False	False		NaN	False
O-151	1[redacted]02	False	False	False	False	False	8888、1723、8181、23	False	False

IP List
(IP_mmdd.csv)

risk_checker.py

leak_checker.py

Result
(IP_mmdd_out.csv)

ip_leak_db.csv