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

Keisuke Tanaka
Ritsumeikan Univeristy,TrendMicro Inc
Saitama, Japan
email:ktanaka@cysec.cs.ritsumei.ac.jp

Soma Sugahara
Ritsumeikan University
Shiga, Japan
email:sugahara@cysec.cs.ritsumei.ac.jp

Yuuki Kimura
Ritsumeikan Univeristy
Shiga, Japan
email:ykimura@cysec.cs.ritsumei.ac.jp

Tetsutaro Uehara
Ritsumeikan University
Shiga, Japan
email:t-uehara@fc.ritsumei.ac.jp

***Abstract*— The recent surge in cyberattacks and data breaches poses a significant threat to Small and Medium-sized Enterprises. In this study, we defined five assessment items and checked companies Global IP addresses, external services and Secure Sockets Layer (SSL)-VPN devices—common entry points for cyber threats. We evaluated 83 companies. In the results, 11 companies (13%) had security risks. Our research methodology could visualize and confirm the existence of companies at risk. This study will hopefully help companies increase their security awareness and improve their security.**

Keywords Security measures; SMEs; Attack Surface Management; ASM.

I. INTRODUCTION

In companies and organizations, the use of client computer and server machines for Internet and internal network connections is fundamental for conducting business activities. In this environment, security incidents occur regularly, such as cyberattacks with the objectives of monetary gain and information theft. Attacks using malicious programs known as 'ransomware' have been particularly frequent recently. It is reported that direct intrusion into an external service, including Virtual Private Network (VPN) devices and server remote desktops, accounts for 81% of the entry points for ransomware attacks [1].

In the authors' previous research, interviews and analysis of interview data were conducted to understand and organize the current status and challenges of cybersecurity measures in Small and Medium-sized Enterprises (SMEs). The previous research findings suggest that, to implement their company's security measures, individuals responsible should have a sense of urgency regarding the current measures, analyze their company's security situation, and adopt an attitude of seeking an objective perspective. These aspects of 'accurate understanding of the current state' are considered crucial for enhancing security measures [2][3].

For SMEs, specific methods to encourage the 'accurate understanding of the current state' of security measures from external sources may include security assessments through interviews and identification and visualization of vulnerable IT assets by using diagnostic tools or Intrusion Detection System (IDS) among other approaches. However, all these methods often come with significant costs. Therefore, there is a need to determine whether mechanisms or initiatives can be established to cost-effectively visualize security risks for SMEs and encourage actions toward improving security measures in these SMEs.

II. SUMMARY OF STUDY

In this study, we defined five assessment items and checked companies' Global IP address, external services, and Secure Sockets Layer (SSL)-VPN devices. These are common entry points for cyber threats, including recent ransomware attacks. We evaluated 83 SMEs in collaboration with the Osaka Chamber of Commerce and Industry (OCCI). The objective, research question, and contribution of this study are as follows.

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

(2) Research Question
- To what extent do external services with a real risk of cyberattacks actually exist?

(3) Targeted Contribution
- Information security personnel in SMEs.

(4) Contribution Details
- The research results and methodology can serve as a reminder and reference for improving a company's own security measures.

 ISBN: 978-1-68558-133-6

III. RELATED WORK

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. The Ministry of Economy, Trade, and Industry of Japan has released introductory guidance [4] on its adoption. 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. Additionally, several information security companies offer ASM services [5][6], but these services are naturally fee-based and encompass a wide range of investigation areas and items, such as domain and email address investigations and investigations of leaked data on the dark web. While these services offer comprehensiveness, they may be overly extensive for SMEs to undertake as their initial security risk assessment.

In this study, our objective is to 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.

IV. RESEARCH METHOD

A. Recruitment of Participating Companies

From May to July 2023, the OCCI recruited participating companies through a webpage under the pretext of a 'Free Security Risk Assessment.' As a result, 83 companies applied, and 156 global IP addresses became the target of the investigation (TABLE 1).

TABLE 1. 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

B. Distribution of Characteristics of Surveyed Companies

The characteristics and distribution of surveyed companies are detailed in TABLES 2, 3, and 4. Approximately 80% had fewer than 100 employees, and 70% had information system personnel.

TABLE 2. 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 or more	4	5%

TABLE 3. PRESENCE OF INFORMATION SYSTEMS PERSONNEL

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

TABLE 4. 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%

 ISBN: 978-1-68558-133-6

C. Investigation Methodology

The investigation of the external service targeted for the survey was conducted by manually importing the list of global IP addresses entered by participating companies into a system created by the authors (Figure 1). Although there are plans to automatically generate reports describing survey results in the future, the reports were manually created this time.

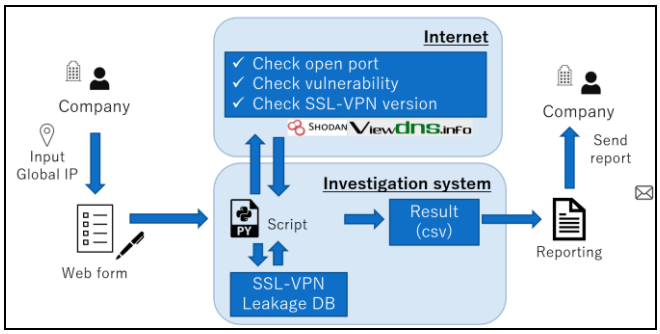

Figure 1. Illustration of the overall process of our methodology.

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

The reason these items were selected is that when an attacker conducts a cyberattack against an external service from the outside, the attacker commonly first attempts to identify the open ports and types of services and then compromises them using vulnerabilities or ID/passwords. Therefore, it is reasonable to check if frequently exploited ports are open (item 1) and if vulnerabilities exist in the ports or services (item 2). Ideally, it would be better if all ports could be checked to determine whether they are open or not, but we did not do that because it is the domain of paid security services provided to specific companies, and the purpose of this study is to efficiently assess the current status of SMEs.

Items 3 and 4 were specific to Fortigate, an SSL-VPN device that is frequently mentioned in recent ransomware incidents and were checked against account leak information and version information. Of course, it would be better if we could investigate SSL-VPN devices from all vendors, but this time we focus on Fortigate, which is frequently abused and has a high market share.

In item 5, we checked for services that seem to pose no risk in terms of port numbers or vulnerabilities, but which allow access to information that should not be disclosed to the outside world. While a one-way check from the outside cannot tell if a company "intends" to disclose such information, the relationships that OCCI has established with each company enable us to check all information to see if it is "intended" to be disclosed or not. The details of these five points are elaborated below.

1) Open Ports with Risks

We confirmed the status of open ports associated with the surveyed global IP addresses, with a primary focus on the status of ports commonly exploited by cyber attackers for intrusion. The target ports included the Remote Desktop (RDP) (3389/Transmission Control Protocol (TCP)), which is frequently abused as an entry point for ransomware, as well as the top two ports frequently abused in various cyberattacks, Secure shell (SSH) (22/TCP) and Telnet (23/TCP) [7], and Server Message Block (SMB) (445/TCP), which was abused by the notorious ransomware 'WannaCry' in the past and continues to be observed as a target.

- 3389/TCP (RDP/Remote Desktop)
- 445/TCP (SMB/File Sharing)
- 22/TCP (SSH/Remote Connection)
- 23/TCP (Telnet/Remote Connection)

We used a web service called ViewDNS [8] to check the status of open ports. ViewDNS offers various verification functions, and one of them is the 'Port Scanner,' which allows the status of open ports to be checked for a given IP address. ViewDNS provides an API, and in this study, we used the API to check the results through the investigation script.

2) Vulnerabilities in Open Ports

The presence of vulnerabilities in open ports associated with the surveyed global IP addresses and the services linked to those ports was investigated using Shodan [9]. Shodan is a service that crawls Internet services, collects information such as open ports, associated service versions, and vulnerabilities, and visualizes the information. In this survey item, we checked whether vulnerability information existed for the surveyed global IP addresses on Shodan.

3) SSL-VPN with Leaked Authentication Information

In September 2021, passwords for 500,000 accounts of Fortinet's SSL-VPN devices, known as Fortigate, were leaked on a hacking forum [10]. We compared the list of IP addresses affected by this public disclosure [11] with the global IP addresses surveyed in this research. We want to expand our research to other SSL-VPNs excluding Fortigate, but we cannot obtain leaked lists on other SSL-VPNs, so in this study, we focus on Fortigate.

4) Outdated Versions of SSL-VPN (Fortigate)

For the surveyed global IP addresses, we accessed the ports used for Fortigate management (443, 8443, 10443, 4443, 4433) to check if a response was obtained. If a response was received, we inferred version information from the response and verified whether the latest firmware version (FortiOS) was in use. This item also focuses only on Fortigate.

 ISBN: 978-1-68558-133-6

5) Unnecessary Exposure of External Access

We accessed the open ports of the surveyed global IP addresses via Hyper Text Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) using a web browser to visually confirm if any web pages were displayed that appeared to be unnecessary for external public access and posed a risk. Risk was determined on the basis of two factors: the presence of login screens or input forms on web pages and the presence of information that appeared to be internal corporate data.

V. RESULTS

A. Summary of Results

In the survey results, 11 companies (13%) had their global IP addresses in a state of security risk. Furthermore, since three companies had security risks in two or more survey items, the survey results of these 11 companies (A-K) are summarized in TABLE 5.

1. Open Ports with Risks: 5
2. Vulnerabilities in Open Ports: 5
3. SSL-VPN with Leaked Authentication Information: 0
4. Outdated Versions of SSL-VPN (Fortigate): 2
5. Unnecessary Exposure of External Access: 3

Note that the names A-K are not related to actual company names but were randomly assigned.

TABLE 5. SUMMARY OF COMPANIES WITH SECURITY RISKS

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

Subsequently, we will provide the survey results for each investigation item. Note that most percentages mentioned in the following sections are based on the total number of companies (83) as the denominator, rather than the total number of IP addresses (156).

1. Open Ports with Risks

Five companies (6%) were found to have open ports with security risks. However, the initially expected opening of Remote Desktop Port (3389/TCP) and File Sharing (445/TCP) was not confirmed (TABLE 6).

TABLE 6. CONFIRMATION RESULTS OF OPEN PORTS

	3389	445	22	23
Port Open	0	0	3	2
Port Closed	83	83	80	81
Percentage	0%	0%	3.6%	2.4%

2. Vulnerabilities in Open Ports

Vulnerabilities were found in five companies (6%). When vulnerabilities are identified on the global IP addresses under investigation using Shodan, an identifier called Common Vulnerabilities and Exposures (CVE) is output to identify the vulnerability. However, due to the large number of detections, they cannot all be listed in a table, so only the number of vulnerabilities is listed in TABLE 7. 'ID' is a unique identifier assigned to the 156 global IP addresses under investigation.

TABLE 7. RESULTS OF VULNERABILITY PRESENCE CONFIRMATION

ID	Vulnerability
O-020	50
O-028	167
O-084	1
O-126	51
O-135	47

3. SSL-VPN with Leaked Authentication Information

Twelve companies (14%) had global IP addresses associated with Fortigate. However, in the scope of this investigation, no matches were found with the list of IP addresses that have had authentication information leaked in the past.

4. Outdated Versions of SSL-VPN (Fortigate)

For 12 companies (14%) out of the 83 with Fortigate IP addresses, the FortiOS version information was retrieved from responses information (TABLE 8). Additionally, the release date of FortiOS versions and the number of days elapsed since then were recorded, using July 31, 2023, as the reference date, which is the closing date for the security risk investigation. The release dates for each FortiOS version were obtained from Fortinet's official documentation. As a result, two companies (16%) had versions that were over a year old, six companies (50%) had versions that were over six months old, and four companies (33%) were using relatively newer versions (TABLE 9).

 ISBN: 978-1-68558-133-6

TABLE 8. FORTIGATE VERSION AND ELAPSED TIME

ID	Ver.	Release	Elapsed Time
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

*O-075 and O-081 are the same company; therefore, the ratio is calculated as one company.

TABLE 9. FORTIGATE VERSION AND ELAPSED TIME (PERCENTAGE)

Elapsed Time	company	percentage
Over one year (365-)	2	16%
Over half a year (183-364)	6	50%
Under half a year (-183)	4	33%

5. Unnecessary Exposure of External Access

Three web service pages (3.6%) were identified as potentially unnecessarily exposed and posing a security risk. The respective companies for each case were contacted and were provided guidance to take measures such as changing the exposure scope to internal-only.

- Cybozu Office Administrator Page
- Trac Lightning
- Kibana

B. Results for Research Question

We asked the following Research Question: To what extent do external service with a real risk of cyberattacks actually exist?

- In this study, 11 companies (13%) had an external service (IP addresses) with security risks.
- However, no matches were found between IP addresses with direct links to recent ransomware attacks, such as the opening of Remote Desktop (3389/TCP) or File Sharing (445/TCP), and IP addresses of SSL-VPN devices that had been leaked in the past.

C. Additional Investigation

Regarding the companies that maintain the surveyed global IP addresses with external services for investigation items 1 and 5 and for which permission to contact was obtained, additional verification was conducted to determine if cyber attackers could successfully authenticate themselves using commonly used IDs and passwords. We tried only 12 patterns of IDs and passwords based on information about which passwords are frequently used [12]. We focus on only easy and frequently used IDs and passwords (TABLE 10) because if we conduct brute force attacks with numerous amounts of IDs and passwords, the companies may be locked out of the external services and have to reset passwords by themselves or have to contact their IT partners.

From the results, it was found that on one webpage, cyber attackers were able to authenticate themselves successfully by using commonly used IDs and passwords (TABLE 11). The relevant company was immediately contacted, and the issue has already been addressed.

TABLE 10. IDS/PASSWORDS USED IN ADDITIONAL INVESTIGATION

ID	Password
admin	blank
admin	admin
admin	password
admin	123456
admin	123456789
admin	1qaz2wsx
root	blank
root	root
root	password
root	123456
root	123456789
root	1qaz2wsx

TABLE 11. RESULTS OF ADDITIONAL INVESTIGATION

Target	Company	Result
SSH	3	No Problem
Telnet	1	No Problem
Web page	2	1 has problem

D. Survey of Companies about this Investigation

After the completion of the investigation and communication of the results, we surveyed the 83 companies regarding the investigation details and findings. Responses were received from 37 companies (44%). These results may be referred to as reflecting the reality of security in SMEs. The results are presented below.

Q1. Did this investigation prove useful?

Thirty-six companies (97%) indicated that the investigation was either "very useful" or "useful."

- Very useful: 19
- Useful: 17
- Not very useful: 1

Q2. Were the investigation results easy to understand?

Thirty-five companies (95%) found the investigation results to be either "very easy to understand" or "easy to understand."

- Very easy to understand: 12
- Easy to understand: 23
- Difficult to understand: 2

Q3. What security concerns or challenges do you have? (Multiple answers allowed)

The most common response was "Uncertainty about whether current security measures are sufficient" (TABLE 12).

TABLE 10. SECURITY CONCERNS

Item	Count	Percentage
Uncertainty about whether current security measures are sufficient.	18	28%
There are things that need to be done, but it's unclear where to start.	4	6%
Uncertainty about what actions to take.	4	6%
Unable to allocate budget for security.	12	19%
Unable to allocate time and personnel for security measures.	10	16%
No specific concerns or challenges.	9	14%
Other.	7	11%

Q4. Were there any areas for improvement identified during the investigation?

The six companies that answered “Yes” were those to whom we had provided improvement recommendations in the report.

- Yes: 6 companies
- No: 31 companies

Q5. (Only asked to the six companies answering ‘Yes’ to Q4)

Were there any aspects of the investigation report that were difficult to understand?

One company responded that they wanted more specific information on what actions to take.

Q6. (Only asked to the six companies answering ‘Yes’ to Q4)

Did you implement security measures on the basis of the investigation results?

- Yes: 3 companies (50%)

Q7. What security measures did you implement?

The three companies answering ‘Yes’ to Q6 implemented the following security measures:

- Blocked specific ports and services.
- Strengthened authentication for specific ports and web services.
- Conducted updates for the operating system and applications.

Q8. Why did you choose not to implement security measures?

The three companies answering “No” to Q6 provided the following reasons for not implementing security measures:

- Understood what needed to be done, but it was costly and time-consuming.
- Planned to implement, but had not completed it yet.
- Did not understand why the measures needed to be implemented.

VI. POSSIBLE IMPROVEMENTS

The following improvements should be implemented for future works.

(1) Selection of Surveyed Companies

In this study, the surveyed companies were those that volunteered for the security risk investigation. Therefore, these companies may possibly have a higher awareness of security and better security measures than typical SMEs. In the future, we will consider expanding the pool of surveyed companies, and consider about how to include companies who have lower awareness of security.

(2) Detailed Situation Assessment

In this investigation, security measures and challenges were not assessed in detail on the basis of the survey results. Therefore, we are considering conducting surveys and interviews on the basis of the investigation results, to gain a more comprehensive understanding of security measures and challenges.

(3) Automation of the Investigation and Report Generation

In this investigation, an automated system was developed for three out of the five investigation items, while manual investigation was conducted for the remaining two items. Additionally, report generation and communication were handled manually. In the future, we will explore the

 ISBN: 978-1-68558-133-6

possibility of automating all investigation items as well as report generation and communication.

VII. CONCLUSION

In this research, 11 out of 83 SMEs (13%) were found to have security risks, but no risk was found directly related to recent ransomware attacks. Our research methodology could visualize and confirm the existence of companies at risk.

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", and 50% of companies who obtained a report have implemented security measures on the basis of the report.

In the future, we will consider improvements, such as better recruitment methods and further automation to make this research method more widely available, like creating a web service for each company to access. We should consider interviewing people at selected companies to gain more background and insight into SMEs security status. We hope that the findings of this study will assist security personnel in SMEs and business owners in enhancing their security measures.

ACKNOWLEDGEMENT

This research would not have been possible without the support and cooperation of many individuals and organizations. We extend our heartfelt gratitude to Mr. Furukawa, Mr. Noda, and Ms. Tosaka from the Osaka Chamber of Commerce and Industry, who not only endorsed the research's objectives but also played a pivotal role in planning the security risk investigation. Their invaluable guidance and support have been instrumental in the success of this study.

We would also like to express our sincere appreciation to all the companies that participated in the diagnostic process. Their willingness to engage in this research and provide essential insights has been integral to its success.

This research project has benefited greatly from the collaboration and contributions of numerous individuals and entities. We extend our deepest thanks to all those involved.

REFERENCES

[1] National Police Agency, "Cyber Threats in the Cyber Space in Reiwa 4th Year" https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf, 2023/3/16.

[2] K. Tanaka, T. Uehara, Y. Furukawa, and M. Noda, "Interview Survey on Information Security Measures in Small and Medium-sized Enterprises," Research Report on Internet and Operation Technology (IOT), 2022-IOT-56, No. 43, pp. 1-8, 2022-02-28.

[3] K. Tanaka, T. Uehara, Y. Furukawa, and M. Noda, "Extraction of Information Security Issues in Small and Medium-sized Enterprises - Interview Analysis Using M-GTA," IEICE Technical Report, vol. 122, no. 85, IA2022-12, pp. 67-70, 2022-06-16.

[4] Ministry of Economy, Trade and Industry, "ASM (Attack Surface Management) Introduction Guidance" https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf, 2023/5/29.

[5] Soliton Systems Co., Ltd., "Supply Chain Security Risk Investigation Service" https://www.soliton.co.jp/news/2022/004703.html, 2022/3/2.

[6] UBsecure Co., Ltd., "Attack Surface Investigation Service" https://www.ubsecure.jp/assessment/attack-surface-assessment, As of March 7, 2024.

[7] National Institute of Information and Communications Technology, "NICTER Observation Report 2022" https://www.nict.go.jp/press/2023/02/14-1.html, 2023/02/14.

[8] View DNS, "Port Scanner" https://viewdns.info/portscan/, As of March 7, 2024.

[9] Shodan, "Shodan Search Engine" https://www.shodan.io/, As of March 7, 2024.

[10] Bleeping Computer, "Hackers leak passwords for 500,000 Fortinet VPN accounts" https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/, 2021/9/8.

[11] GitHub, "Fortinet Victim List" https://gist.github.com/crypto-cypher/f216d6fa4816ffa93c5270b001dc4bdc, As of March 7, 2024.

[12] Nordpass, “Most Common Password list” https://nordpass.com/most-common-passwords-list/, As of March 7, 2024.

 ISBN: 978-1-68558-133-6