Vulnerability Assessment: A Proof of Concept

Madihah Mohd Saudi[1], Mohd Haizam Saudi[2], Obsatar Sinaga[3], Azuan Ahmad[4], Muhammad 'Afif Husainiamer[5]

[1]Islamic Science Institute (ISI), Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
[2]Widyatama Universiti, Bandung, Indonesia
[3]Padjadjaran University, Indonesia
[4]Islamic Science Institute (ISI), Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
[5]Faculty of Science & Technology (FST), Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
*madihah@usim.edu.my

ABSTRACT

Cybercrime attacks are not just harmful to data privacy and data security, they also pose a threat to the performance, monetary and reputation of many different organizations. Due to the rapid growth of cybercrime attacks especially in e-commerce, e-governance, e-learning, and various other e-services, there is a rising problem where databases are easily obtained and misused. Data breach and exploitation are highly related to the threat and vulnerability in a system or application. Hence, this paper presents a Proof of Concept (POC) that is related to data breach and data exploitation. Based on the POC, we have developed a formula for general vulnerability assessment, which can be used as a guide for any organization with the same interest.

Keywords
Vulnerability assessment, data privacy, data security, proof of concept (POC), malware

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

Introduction

According to [1], people should keep their information safe and secure from third-party interventions to prevent a form of a data breach. Cybercrime is known as a criminal way of doing an activity using digital devices and the internet such as internet scams, online harassment, cross-site scripting, and identity theft by a group of people [2]. The number of cases of cybercrime in the world is increasing rapidly day by day. According to the prediction of cybersecurity ventures, cybercrime would cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. The expected cost of cybersecurity is increasingly rising to $170 billion in 2020, which in 2015 was just $75 billion [2]. The confidentiality, integrity and availability (CIA) are often referred to as the CIA Triad. In Cybersecurity, the CIA triad is important because it offers critical security functionality, helps prevent enforcement problems, maintains business continuity, and avoids reputational harm to the company [3]. Since the outbreak of COVID-19, there have been reports of cybercrime attacks, especially that are related to scams impersonating public authorities and organizations, Personal Protection Equipment (PPE) fraud, and offering COVID-19 cures. Work from home (WFH) has increased the level of cybersecurity concerns and challenges never faced before by industry and citizens. Cybercriminals have used this opportunity to expand their attacks and cause on heightened stress, anxiety and worry facing individuals. Besides, the experiences of WFH revealed the general level of unpreparedness by software vendors, particularly as far as the security of their products was concerned [4].

This paper is organized as follows. Section II explains related works, Section III presents the method used in this paper, Section IV consists of the POC findings, and Section V concludes the paper and makes suggestions for future work.

Literature Review

A threat is an action taken to gain a benefit from security breaches in a system and negatively impact it [5]. Examples of cybercrime attacks are malware, spyware, phishing attacks, DDoS attacks, ransomware, and Trojan. All these threats are common face by any organization. Vulnerabilities are flaws in a system or its design

that allows an attacker to execute malicious commands, access data in an unauthorized way, or conduct various denial-of-service attacks. A combination of both threats and vulnerabilities actually can lead to risk [6]. Risk is a function of threats exploiting vulnerabilities to obtain, damage, or destroy assets. Thus, threats may exist, but if there are no vulnerabilities then there is no risk. Risk usually will affect an organization by either cause it to temporary or permanent disruption. Data types for the data input that will be used in CVE. CVE stands for Common Vulnerabilities and Exposures. The Common Vulnerabilities and Exposures system provides a reference-method for publicly known information-security vulnerabilities and exposures. CVE is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services. As such, CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with a status indicator, a brief description, and references to related vulnerability reports and advisories. From the CVE itself, we will able to know what kind of vulnerabilities and the solution for it.

The data preparation process starts with data collection obtained from two sources (threat and vulnerabilities). Data collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions and evaluate outcomes. The data collected then undergo a cleaning process. Data cleaning also referred to as data cleansing is one of the most important steps to create a culture around quality data decision-making. Data cleaning is the process of fixing or removing incorrect, corrupted, incorrectly formatted, duplicate, or incomplete data within a dataset. When combining multiple data sources, there are many opportunities for data to be duplicated or mislabeled. If data is incorrect, outcomes and algorithms are unreliable, even though they may look correct. There is no one absolute way to prescribe the exact steps in the data cleaning process because the processes will vary from dataset to dataset. While the techniques used for data cleaning may vary according to the types of data. The process continues with data correlation after the cleaning process. Correlations are useful for describing simple relationships among data without making a statement about cause and effect. Table 1 shows the type of data sources for the different event types. While, Table 2 summarized the CVE exposure.

Table 1. Data sources

Event Type	Data Source
Network trace (NT)	Raw packets
	Netflow
Security events (SE)	Intrusions detection systems
	Firewalls
	Virtual private networks
	Anti-virus
Network activity context (NAC)	Proxy servers
	Layer 7 application context
User/asset context (UC)	Vulnerability scanners
Network events (NE)	Switches
	Routers
	Servers
	Hosts
Virtualization infrastructures (VI)	Open stack
	Microsoft Hyper-V
	VM Ware
Non- log information (NLI)	HR Databases
	User locations
	Software inventory

	WHOIS records (Database of known malicious IPs) (Configuration management database)
Application logs (AL)	Databases Operating systems

Table 2. Common vulnerability exposure

Affected Product or Software	Version	Vulnerability	How Do Attackers Exploit This Vulnerability?	Impact	Solution
• VMware Workspace One Access (Access) • VMware Workspace One Access Connector (Access Connector) • VMware Identity Manager (vIDM) • VMware Identity Manager Connector (vIDM Connector) • VMware Cloud Foundation • vRealize Suite Lifecycle Manager	VMSA-2020-0027.1	Command Injection Vulnerability	An attacker with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account can execute commands with unrestricted privileges.	Allowed malicious actors to execute commands with unrestricted privileges.	Apply an update
Replay Protected Memory Block (RPMB) protocol as specified in multiple standards for storage device interfaces, including eMMC, UFS, and NVMe.	WDC-20008	• Vulnerable to replay attacks. • Denial Service	An attacker with physical access can deceive a trusted component about the status of an RPBM write command or the content of an RPMB area.	• Caused a mismatch between the write state or contents of the RPMB area and a trusted component of the device. • make the trusted component believing a write command failed when in fact it succeeded,	Apply an update
Macrium Reflect	v7.3.52	Vulnerable to	Because unprivileged	Able to execute	Apply an

	81	privilege escalation due to OPENSSLDIR location	Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges.	arbitrary code with SYSTEM privileges on a Windows system with the vulnerable Macrium software installed.	update
Chocolatey Boxstarter	version 2.13.0	Vulnerable to privilege escalation due to weak ACLs	Place a DLL in this directory that a privileged service is looking for.	Can execute code with SYSTEM privileges. (privilege escalation)	Apply an update
Acronis Cyber Backup	V12.5	Multiple privilege escalation vulnerabilities	By placing a specially-crafted openssl.cnf or DLL file in a specific location, an unprivileged user may be able to execute arbitrary code with SYSTEM privileges on a Windows system with the vulnerable Acronis software installed.	Allow an unprivileged Windows user to be able to run arbitrary code with SYSTEM privileges.	Apply an update
Microsoft Windows Netlogon Remote Protocol (MS-NRPC	V36.0	• Unauthorized access. • denial of service	By choosing a client challenge and ClientCredential of all zeros, an attacker has a 1 in 256 chance of successfully authenticating as any domain-joined computer. By impersonating a domain controller, an attacker can take additional steps to change a computer's Active Directory password and potentially gain domain administrator privileges	• Can impersonate any domain-joined computer, including a domain controller. • Can set an empty password for the domain controller's Active Directory computer account, causing a denial of service • Allowing the attacker to gain domain administrator privileges.	Apply an update

IPTV/H.264/H.265	IPTV/H.264/H.265	• Unauthorized access. • denial of service	The underlying software in these devices seems to share common components that have multiple weaknesses in their design and default configuration.	• Full administrative access via backdoor password (CVE-2020-24215) • Administrative root access via backdoor password (CVE-2020-24218) • Arbitrary file read via path traversal (CVE-2020-24219) • Unauthenticated file upload (CVE-2020-24217) • Arbitrary code execution by uploading malicious firmware (CVE-2020-24217) • Arbitrary code execution via command injection (CVE-2020-24217) • Denial of service via buffer overflow (CVE-2020-24214) • Unauthorized video stream access via RTSP (CVE-2020-24216)	Restrict network access. Apply updates
Devices supporting both Bluetooth BR/EDR and LE	versions 4.2 and 5.0	• Man in the Middle (MITM)	Attacker pairing over BR/EDR or LE and overwriting an existing	Several potential attacks could be performed by	Conformance tests to ensure that the

using Cross-Transport Key Derivation (CTKD)		attack • Unauthorized access	LTK or LK on the other transport. When this results in the reduction of encryption key strength or the overwrite of an authenticated key with an unauthenticated key, the attacker could gain additional access to profiles or services that are not otherwise restricted.	exploiting CVE-2020-15802, including a Man in the Middle (MITM) attack and BLUR attacks	overwrite of an authenticated key or a key of a given length with an unauthenticated key or a key of reduced length is not permitted in devices supporting Bluetooth Core Specification version 5.1 or greater -restrict the duration of pairing mode
Diebold Nixdorf 2100xe USB automated teller machines (ATMs)	version 1.1.30	• vulnerable to physical attacks	The attacker must first deposit actual currency and modify messages from the CCDM to the host computer to indicate a greater amount or value than was deposited. Then the attacker must make a withdrawal for an artificially increased amount or value of the currency. This second transaction may need to occur at an ATM operated by a different financial institution	Able to commit deposit forgery	-Obtain advice from the vendor. -Apply an update -Consider additional countermeasures
NCR SelfServ automated teller machines (ATMs	APTRA XFS 04.02.01 and 05.01.00	• vulnerable to physical attacks	The attacker must first deposit actual currency and modify messages from the CCDM to the host computer to indicate a greater amount or value than was deposited. Then the attacker must make a withdrawal for an artificially increased amount or value of the currency. This second transaction may need to	Can execute arbitrary code and able to commit deposit forgery	-Apply an update

	occur at an ATM operated by a different financial institution

Next, the computer has to learn how to make a prediction, so it uses the collected data to create something called a model. From the model, we can predict a new type of attack, pattern, or algorithm of cybersecurity attacks. Combining the strength of artificial intelligence (AI) with Cyber Security, security professionals have additional resources to defend vulnerable networks and data from cyber attackers. After applying this technology, it brought instant insights, resulting in reduced response times. AI can analyze user behaviors effectively, deduce a trend, and recognize all kinds of network anomalies or irregularities. The details of the method will be explained in the next section.

Methodology

The overall processes involved in this paper as summarized in Figure 1.

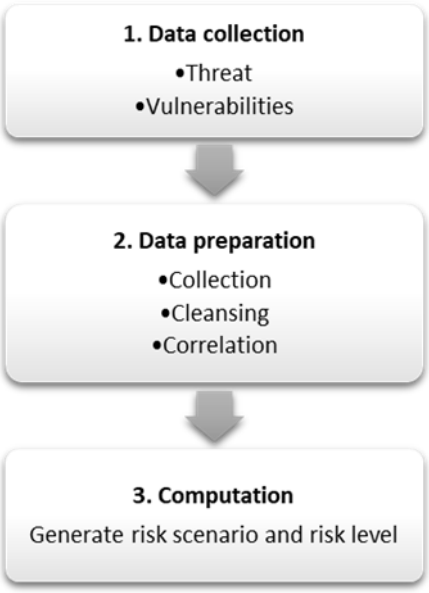

Figure 1. Overall processes

To train the model, based on Table 2, we define the formulation as follows.

A = Affected product
A_1= VMware
A_2 = Replay Protected Memory Block (RPMB) protocol
A_3 = Macrium Reflect
A_4 = Chocolatey Boxstarter
A_5 = Acronis Cyber Backup
A_6 = Microsoft Windows Netlogon Remote Protocol (MS-NRPC
A_7 = IPTV/H.264/H.265
A_8 = Devices supporting both Bluetooth BR/EDR and LE using Cross-Transport Key Derivation (CTKD)
A_9 = Diebold Nixdorf 2100xe USB automated teller machines (ATMs)
A_{10} = NCR SelfServ automated teller machines (ATMs)

B = Version
B_1= VMSA-2020-0027.1
B_2 = WDC-20008
B_3 = v7.3.5281
B_4 = version 2.13.0
B_5 = V12.5
B_6 = V36.0
B_7 = IPTV/H.264/H.265
B_8 = versions 4.2 and 5.0
B_9 = version 1.1.30
B_{10} = APTRA XFS 04.02.01 and 05.01.00

C = Vulnerabilities
C_1= Command Injection Vulnerability
C_2 = Vulnerable to replay attacks
C_3 = Denial Service
C_4 = Privilege escalation
C_5 = Unauthorized access.
C_6 = Man in the Middle (MITM) attack
C_7 = vulnerable to physical attacks

D = How do attackers exploit this vulnerability?
D_1 = Attacker with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account can execute commands with unrestricted privileges.
D_2 = An attacker with physical access can deceive a trusted component about the status of an RPBM write command or the content of an RPMB area.
D_3 = Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a

specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges.

D_4 = Place a DLL in this directory that a privileged service is looking for.

D_5 = By placing a specially-crafted openssl.cnf or DLL file in a specific location, an unprivileged user may be able to execute arbitrary code with SYSTEM privileges on a Windows system with the vulnerable Acronis software installed.

D_6 = By choosing a client challenge and ClientCredential of all zeros, an attacker has a 1 in 256 chance of successfully authenticating as any domain-joined computer. By impersonating a domain controller, an attacker can take additional steps to change a computer's Active Directory password and potentially gain domain administrator privileges.

D_7 = The underlying software in these devices seem to share common components that have multiple weaknesses in their design and default configuration.

D_8 = Attacker pairing over BR/EDR or LE and overwriting an existing LTK or LK on the other transport. When this results in the reduction of encryption key strength or the overwrite of an authenticated key with an unauthenticated key, the attacker could gain additional access to profiles or services that are not otherwise restricted.

D_9 = The attacker must first deposit actual currency and modify messages from the CCDM to the host computer to indicate a greater amount or value than was deposited. Then the attacker must make a withdrawal for an artificially increased amount or value of the currency. This second transaction may need to occur at an ATM operated by a different financial institution

D_{10} = The attacker must first deposit actual currency and modify messages from the CCDM to the host computer to indicate a greater amount or value than was deposited. Then the attacker must make a withdrawal for an artificially increased amount or value of the currency. This second transaction may need to occur at an ATM operated by a different financial institution

E= Impact

E_1 = Allow malicious actors to execute commands with unrestricted privileges.

E_2 = Cause a mismatch between the write state or contents of the RPMB area and a trusted component of the device.

E_3 = make the trusted component believing a write command failed when in fact it succeeded

E_4 = Able to execute arbitrary code with SYSTEM privileges on a Windows system with the vulnerable Macrium software installed.

E_5 = Can execute code with SYSTEM privileges (privilege escalation).

E_6 = Allow an unprivileged Windows user to be able to run arbitrary code with SYSTEM privileges.

E_7 = Can impersonate any domain-joined computer, including a domain controller.

E_8 = Can set an empty password for the domain controller's Active Directory computer account, causing a denial of service

E_9 = Allowing the attacker to gain domain administrator privileges.

E_{10} = Full administrative access via backdoor password (CVE-2020-24215)

E_{11} = Administrative root access via backdoor password (CVE-2020-24218)

E_{12} = Arbitrary file read via path traversal (CVE-2020-24219)

E_{13} = Unauthenticated file upload (CVE-2020-24217)

E_{14} = Arbitrary code execution by uploading malicious firmware (CVE-2020-24217)

E_{15} = Arbitrary code execution via command injection (CVE-2020-24217)

E_{16} = Denial of service via buffer overflow (CVE-2020-24214)

E_{17} = Unauthorized video stream access via RTSP (CVE-2020-24216)

E_{18} =Several potential attacks could be performed by exploiting CVE-2020-15802, including a Man in the Middle (MITM) attack and BLUR attacks

E_{19} = Able to commit deposit forgery

E_{20} = Can execute arbitrary code and able to commit deposit forgery

F = Solution

F_1 = Apply an update

F_2 = Restrict network access

F_3 = conformance tests to ensure that the overwrite of an authenticated key or a key of a given length with an unauthenticated key or a

key of reduced length is not permitted in devices supporting Bluetooth Core Specification version 5.1 or greater

F_4 = restrict the duration of pairing mode
F_5 = Obtain advice from the vendor
F_6 = Consider additional countermeasures

Results and Discussion

For POC, all of the processed data will be utilized to compute the probability of risk occurrence for the next process which is identifying risk level using a risk matrix. A possible risk that can happen related to cybersecurity is a malware attack, DDoS attack, ransomware attack, server failure and firewall penetration. A risk matrix is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity of impact. The impact of each risk can be classified into 5 categories which is not impacted, minimally affected, partially affected, impacted and very impacted. After both the category of probability and the category of consequence severity of impact being mapped, the conclusion can be made whether the risk is low, moderate, noticeable, or high. This is a simple mechanism to increase the visibility of risks and assist management in decision making. Table 3 shows how risk rating and the control measure for each risk based on risk level. Table 4 below shows the example of a risk matrix that needs to be constructed to identify the risk level by mapping both the probability and severity of the risk scenario identified. Table 4 was built based on PESTLE. PESTLE stands for Political, Economic, Social, Technological, Environmental and Legal factors. For this POC, we used PESTLE analysis for the risk assessment process regarding cybersecurity. It is really useful for analyzing and monitoring the macro-environmental factors that may have a profound impact on an organization. [7-12] were the examples of existing works that used PESTLE for risk management.

Table 3. Risk rating and control measure

Product	Risk Rating Probability	X	Parameter of Impact	=	Rating Action Bands Risk Level	Control Measures
A_1	Most likely	X	E_1	=	Minimal risk	F_1
A_2	Unlikely	X	E_2 and E_3	=	Low risk	F_1
A_3	Likely	X	E_4	=	Moderate risk	F_1
A_4	Can happen	X	E_5	=	Minimal risk	F_1
A_5	Most likely	X	E_6	=	Noticeable risk	F_1
A_6	Unlikely	X	E_7, E_8 and E_9	=	Low risk	F_1
A_7	Likely	X	E_{10} ,E_{11}, E_{12}, E_{13}, E_{14}, E_{15}, E_{16} & E_{17}	=	Noticeable risk	F_1 and F_2
A_8	Can happen	X	E_{18}	=	Noticeable risk	F_3 and F_4
A_9	Most likely	X	E_{19}	=	High risk	F_1 F_5 and F_6
A_{10}	Unlikely	X	E_{20}	=	Low risk	F_1

Table 4. POC risk matrix

	Parameter impact				
Different work process	Efficient	Partially efficient	Neutral	Partially not efficient	Not efficient
Expectation of output result from user	Satisfied	Partially satisfied	Neutral	Partially not satisfied	Not satisfied
Accuracy of assumption on threat and vulnerability	Accurate	Partially accurate	Neutral	Partially not accurate	Not accurate
Data consistency	consistent	Partially consistent	Neutral	Partially not consistent	Not consistent

	The next 12 months				Not Important 1	Partially important 2	Neutral 3	Important 4	Very Important 5
Parameters probability	>75%	Most likely it will happen	5	Very High	NOTICEABLE	NOTICEABLE	HIGH	HIGH	HIGH
	50%-70%	Expected to happen	4	High	MODERATE	NOTICEABLE	NOTICEABLE	HIGH	HIGH
	25%-<50%	Can happen	3	Moderate	LOW	MODERATE	NOTICEABLE	HIGH	HIGH
	10%-<25%	It may happen	2	Low	LOW	LOW	MODERATE	NOTICEABLE	HIGH
	<10%	May not happen	1	Very Low	LOW	LOW	MODERATE	NOTICEABLE	NOTICEABLE

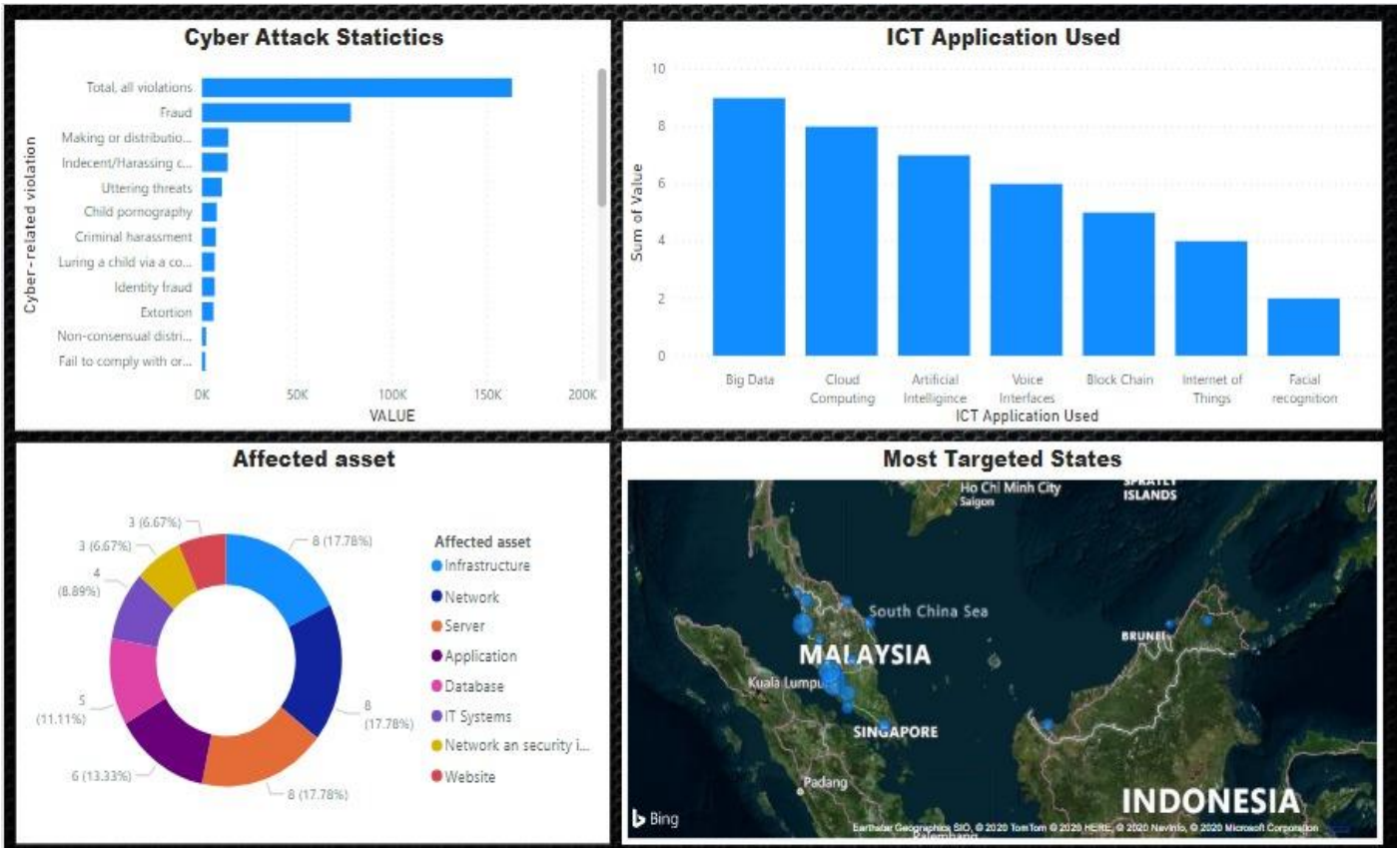

Figure 2. Visualization of the vulnerability assessment

Figure 2 showed the visualization from Table 1 and Table 2, which are correlated with Table 3 and Table 4.

Conclusion

Based on the POC we presented, we came out with a formulation for vulnerability assessment with the integration of PESTLE analysis. Our work is very beneficial for end-users and organizations in mitigating cybercrimes attacks. This is part of knowledge sharing and can be used as guidance for law enforcement or research center in assessing vulnerability at their organizations.

References

[1] Othman, N. (2020). Information Privacy Awareness Among Young Generation in Malaysia. Journal of Science, Technology and Innovation Policy, 5(2).

[2] P. Thangamuthu, A. Rathee, S. Palanimuthu, and B. Balusamy, "Cybercrime," in Encyclopedia of Criminal Activities and the Deep Web. IGI Global, 2020, pp. 1–22.

[3] Hoffman, L., & Zahadat, N. Securing Democracy: A Comparative Look at Modern and Future US Voting Systems Through the Lens of the CIA Triad. Journal of Information Assurance and Security, 13, 118-124.

[4] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.

[5] Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 2020, 1-19.

[6] In, H. P., Kim, Y. G., Lee, T., Moon, C. J., Jung, Y., & Kim, I. (2004). A security risk analysis model for information systems. Asian Simulation Conference, pp. 505-513.

[7] Serfointein, E., & Govender, K. K. (2020). Stakeholders' views regarding macro-environment impacts on commercial flight operations in South Africa. Journal of Transport and Supply Chain Management, 14, 11.

[8] Veerasamy, N., Mashiane, T. T., & Pillay, K. J. (2019). Towards cyber incident response strategic planning.

[9] Mulualem, E. (2019). Developing Cyber Security Risk Assessment Framework for Railways Industry in Ethiopia. PhD thesis, St. Mary's University.

[10] Guzzo, P. P. Cyber-Pharmacies and pharmacists for digital health in post-COVID-19. ESA RN16, 19.

[11] Hentula, M., Sarja, J., & Tuunanen, K. The Threats in AR Cloud. Emerging Technology Adoption and Use, 118.

[12] Lee, S. J. G. (2019). Architecting a secure enterprise with a systems-thinking approach. PhD thesis, Massachusetts Institute of Technology.