CYBER SECURITY INCIDENT REPORT

Name

Institution Affiliation

Course

Instructor

Date

CYBER SECURITY INCIDENT REPORT

1. INTRODUCTION

1.1 This document presents the Colonial Pipeline cyber security incident report in a clear and structured manner to capture some key elements of the attack.

1.2. This report aims to discuss the incident, describe the attack vector, evaluate the consequences of the Colonial Pipeline ransomware attack, and discuss the actions taken by the organization. This report is in the Cyber Security Incident Report Format provided for contractor entities to use when handling classified or sensitive information.

1.3 This paper targets security personnel, national security forces, and other decision-making officials and institutions managing cyber security threats.

2. SCOPE

2.1 This Cyber Security Incident Report follows the guidelines outlined in the Cyber Security Incident Report Format. It is used to educate users about one of the recent ransomware attacks known as the Colonial Pipeline ransomware attack. It can be used as a reference material for understanding cyber security and plans for it.

2.2 The document presents information on the break-in, the type of systems and data affected, measures taken in response to the breach, and the implications on other aspects of the critical infrastructure.

2.3 This document will help national and industrial cyber security strategies by giving a detailed analysis of the attack, types of vulnerability utilized, and suggestions on preventing such an occurrence.

CYBER SECURITY INCIDENT REPORT

1.0 Reported By

1.1Surname:		1.2 Forenames:	
1.3Position:	Cybersecurity Analyst		
1.4 Name of organization or company:	Colonial Pipeline		
1.5 TelephoneNo:			
1.6 E-mail:			

2.0 Organization Details

2.1 Name of organization:	Colonial Pipeline
2.2 Type of organization:	Fuel pipeline operator
2.3 Street Address:	Alpharetta, Georgia, USA
2.4At this time, is it known that other organizations are affected by this incident?(If so, list names, addresses, telephone number, email addresses and contact persons):	Fuel suppliers, airlines, gas stations, and consumers residing in the eastern part of the United States.

3.0 Incident Details including Injury and Impact Level

3.1Date:	May 7, 2021	3.2 Time:	Early morning
3.3 Location of affected site:	Colonial Pipeline Information Technology (IT) network		
3.4 Brief summary of the incident (what has happened, where did it happen, when did it happen):	DarkSide ransomware breached Colonial Pipeline's information technology infrastructure and demanded a ransom.		
3.5 Description of the project/program and information involved, and, if applicable, the name of the Specific program:	Colonial Pipeline, a major supplier of refined oil products across the Eastern U.S.		
3.6 Classification level of the information involved	Sensitive corporate and operational data		
3.7 System compromise (detail):	Unauthorized access and encryption of business IT systems		
3.8 Data compromise (detail):	No concrete evidence showed that the operational control system had been compromised, but corporate IT data was affected.		
3.9 Originatorand/or Official Classification Authority of The information involved? (List name, address,	U.S. Federal Agencies (FBI, CISA)		

telephone no., email and contact person).	
3.10 Is Foreign Government Information involved? Originating country or International organization?	Even though the group has no direct affiliation with any foreign government, it has connections with Russia-based cybercriminals
3.11 Did the incident occur on an accredited system authorized to process and store the information in question?	Yes
3.12 Estimated injury level/sector:	High impact affecting the distribution of fuel and leading to a short supply.
3.13 Estimated impact level: (any compromise or disruption to service?)	Severe. This led to fuel supply interruptions in some areas and emergency measures being taken.
3.14 Incident duration:	Approximately one week before full recovery.
3.15 Estimated number of systems affected:	Multiple corporate IT systems
3.16 Percentage of organization systems affected:	IT systems were fully compromised, and pipeline operations were temporarily shut down.

3.17 Action taken:	Colonial Pipeline offered a $4.4 million ransom, of which the FBI recovered some, hired cybersecurity professionals, and enlisted federal agencies.
3.18 Supporting documents attached (describe if any)	FBI report, forensic analysis
3.19 Multiple occurrence or first time this type of incident Occurs within this location?	First significant ransomware attack on Colonial Pipeline.
3.20 Incident Status (resolved or unresolved)	Resolved.
3.21 Has the matter been reported to other authorities? If so, list names, addresses, telephone no., email and contact person.	Yes, reported to FBI, CISA, and Department of Homeland Security.

4.0 Status of Mitigation Actions

4.1Mitigation details to date: (List any actions that have been taken to mitigate Incident and by whom)	Employed cybersecurity firms, introduced multi-factor authentication protocols, and enhanced network segregation.
4.2Results of mitigation:	Implementing measures made the website more secure against cybercrime, particularly against ransomware.

4.3 Additional assistance required?	Continued monitoring and government collaboration

5.0 Computer Network Defense Incident Type (if applicable)

5.1 Malicious code: (Worm, virus, trojan, Back door, rootkit, etc.)	Ransomware (DarkSide variant)
5.2Known vulnerability exploit: (List the Common Vulnerabilities and Exposures (CVE) number for known vulnerability)	Credential compromise, phishing
5.3 Disruption of service:	Yes, fuel distribution halted
5.4Access violation: (Unauthorized access attempt, successful unauthorized access, password cracking, Etc.)	Unauthorized access by using a stolen account and password.
5.5Accident or error: (Equipment failure, operator error, user error, natural or Accidental causes)	No.
5.6 If the incident resulted	

<table>
<tr><td>from user error or malfeasance, identify reasons (training, disregard for policy, Other) and responsible parties.</td><td colspan="4">DarkSide ransomware group</td></tr>
<tr><td>5.7 Additional details:</td><td colspan="4">Attackers stole 100GB of data before deploying ransomware.</td></tr>
<tr><td rowspan="3">5.8.Apparent Origin of Incident or Attack</td><td>Source IP and port:</td><td>Not publicly disclosed</td><td>Protocol:</td><td>Likely Remote Desktop Protocol (RDP) or phishing attack used to gain initial access</td></tr>
<tr><td>URL:</td><td>No specific URL identified</td><td>Malware:</td><td>DarkSide ransomware, a Ransomware-as-a-Service (RaaS) variant.</td></tr>
<tr><td>Additional details:</td><td colspan="3">DarkSide, a Russian-affiliated criminal gang, hacked into Colonial Pipeline’s computer system, locked the data and demanded a $4.4 million ransom and, in part, the FBI got back.</td></tr>
</table>

6.0 Systems Affected

6.1 Network zone affected: (Internet, administration, internal, etc.)	IT network (administrative and operational coordination systems).
6.2 Type of system affected: (Fileserver, Webserver, mail server, database, workstation (mobile or desktop),etc.)	File servers, network controllers, IT management systems.
6.3 Operating system (specify version):	Windows-based systems.
6.4 Protocols or services:	Security threats in remote access
6.5Application (specify version):	Corporate software and internal systems.

7.0 Follow-on Activities

7.1 Has information contained in this report been provided to the authorities? When?	Yes, the FBI and CISA are involved.
7.2 Next steps as discussed by the security authorities (document here in the event that management or chain of command has not yet been	Increased focus on cybersecurity measures, improved access controls, and industry promotion campaigns.

informed of the incident, or that a status report is required).	

Question 2: Evolution of Cybercrime Over the Last Decade

With the enhanced technological development in the last decade, new unique and complex cybercrimes have been created, placing individuals at a higher risk. New threats like ransomware-as-a-service (RaaS), deepfake scams, and crypto-jacking have made it easier for attackers to launch attacks against targets (Temara, 2024). AI enhances phishing and IoT device hacking as AI empowers smarter socially engineered attacks, and many IoT devices contribute to the potential attack vectors. Unlike traditional crimes, these threats are often committed from a distance, and it is possible to attack entire networks or organizations' databases within minutes.

As more and more people use the Internet in their everyday activities, such as banking, shopping, or communication, more people become vulnerable to identity theft or other malicious activities of cybercriminals (Deora & Chudasama, 2021). It has been established that cybercrime is favored because of the level of anonymity that it offers, as well as the speed and spread that is possible for it. Besides, most people do not have adequate cyber security knowledge and thus are easy targets for scams and hacking. To guard against these threats, institutions and persons must implement better protections such as multi-factor authentication, regular software patches, and training. This way, individuals can become fully aware of the nature and trends of digital criminology and minimize the risks of being victims.

References

Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.

Temara, S. (2024). The Dark Web and Cybercrime: Identifying Threats and Anticipating Emerging Trends. *Authorea Preprints*.