**CS 571 Case Studies in Computer Security team project**

* **Team and Topic**
  1. **Team**: The Rhode Islanders

Humberto Martinez, Justin Cabral, Jonathan Duran, Shary Llanos-Antonio

* 1. **Case Study:** Identify the case study for your team project (victim being attacked)

Colonial Pipeline, which is an American gas company that provides gas to the southern and eastern United States.

**Suggested rewording:** Colonial Pipeline, the major refined products pipeline in the United States, moving daily more than 100 million gallons of fuel (gasoline, diesel, and jet fuel) from Houston, Texas to the New York Harbor.

* 1. **Case Study Significance**: Identify why this case study is significant/interesting to research

This case study is an interesting research topic because it is not only recent, but it affected a major sector of our national security, that being our energy sector. It is a good piece of analysis because we can look at how the private/public partnership between the federal government and private businesses affect their security practices. It will also give us an opportunity to see if the federal government is holding high security standards for the private companies that it depends on to distribute energy around the country.

**Suggested rewording:** The Colonial Pipeline case is significant as a ransomware attack on the critical infrastructure of the United States. It raises technical concerns about cybersecurity hygiene, as the attackers used a leaked password to access their network through a legacy VPN system [1].

Also, it will allow us to analyze how the private/public partnership between the federal government and private companies affects their security practices. Furthermore, it will enable us to see if the federal government holds high-security standards for the private companies that it depends on to distribute energy around the country.

[1] Kelly, S., & Resnick-ault, J. (2021, June 8). *One password allowed hackers to disrupt colonial pipeline, CEO tells senators*. Reuters. Retrieved January 21, 2022, from <https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-wer e-compromised-ahead-hack-2021-06-08/>

* 1. **Collaboration Timing**: Summarize the timing you have worked out for collaboration (e.g., days/times)

Monday – Friday, mornings until 12.

* 1. **Collaboration Techniques**: Summarize the techniques you have worked out for collaboration (e.g., tools)

One of the tools we will be using to collaborate with each other will be Microsoft Teams, which is an excellent communication platform that allows the sharing of files and screens so that team members can work together effectively. We will also be using many of the Microsoft Office 365 suite applications such as Word and PowerPoint to create some of the graphs or visual representations and obviously to write our project reports.

* **Contribution Agreement**: Identify how each member of the team will contribute to the project using a matrix with the following information:
  + Columns = roles
  + Rows = assignment pieces for report sections, final report, and final presentation
  + Cells = name of team member

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Book Boss** | **Primary Author** | **Primary Editor** | **Secondary Author** |
| **Team Report 1** | Justin | Humberto | Jonathan | Shary |
| **Team Report 2** | Humberto | Jonathan | Shary | Justin |
| **Final Report (Part 3)** | Jonathan | Shary | Justin | Humberto |
| **Final Presentation** | Shary | Justin | Humberto | Jonathan |

**Possible References for Team Report Part 1 due on Week 5**

Smith, M. and Monken, J., 2021. *The Colonial Pipeline Hack Shows We Need a Better Federal Cybersecurity Ecosystem - Modern War Institute*. [online] Modern War Institute. Available at: <https://mwi.usma.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem> [Accessed 20 January 2022].

Sanger, D. and Perlroth, N., 2021. *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*. [online] Nytimes.com. Available at: <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html> [Accessed 20 January 2022].

Internet Crime Complaint Center (IC3). (2021, May 11). *Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*. [online] IC3.gov. Available at: <https://www.ic3.gov/Media/News/2021/210520.pdf> [Accessed 20 January 2022]

Parfomak, P. W., & Jaikaran, C. (2021, May 11). *Colonial Pipeline: The darkside strikes*. [online] Congressional Research Service (CRS) for the United States Congress. Available at: <https://crsreports.congress.gov/product/pdf/IN/IN11667> [Accessed 20 January 2022]

Shah, S. (2022, January 6). *The colonial pipeline attack eight months on*. [online] Infosecurity Magazine. Available at: <https://www.infosecurity-magazine.com/opinions/the-colonial-pipeline-attack-eight/> [Accessed 20 January 2022]

FBI. (2021, May 10). *FBI statement on Compromise of Colonial Pipeline Networks.* [online]. Available at: <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks> [Accessed 20 January 2022]

Kelly, S., & Resnick-ault, J. (2021, June 8). *One password allowed hackers to disrupt colonial pipeline, CEO tells senators*. Reuters. [online]. Available at:, from https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

Ransomware Impacting Pipeline Operations : <https://www.cisa.gov/uscert/ncas/alerts/aa20-049a>