2023 Discord-Pentagon Data Breach

Alexander Kellough

April 16, 2023

Data leaks and breaches seem like common occurrences in the modern cybersecurity landscape, and many people undergo irreparable damage because of these. However, no breaches seem so dangerous as those affecting nation-states. In the past two weeks at time of writing, there has been a large amount of new circulation concerning a data breach/leak involving U.S. classified documents ranging in scope and topic. The argument will be made that this leak was either preventable, or mitigatable, by the proper implementation and enforcement of policies and procedures.

# Chain-of-Events:

In April of 2023, a set of classified U.S. government documents began to circulate around social media website 4chan. Among these documents were files detailing intelligence on the Russo-Ukrainian war, as well as appraisals of U.S. allies and rivals. The leaks were eventually traced to a chatroom on the popular social media app Disord, that was devoted to the videogame Minecraft.

According to The Washington Post, the origin point for the leak has been traced to a Discord Server named “Thug Shaker Central”, where members would meet to talk about a wide array of topics, from geopolitics, to crude, and sometimes offensive humor. The main perpetrator of the incident was 21-year-old Jack Teixeira, who worked in IT at the Otis Air National Base in Cape Cod Massachusetts. Teixeira went by “O.G” in the discord server, where he spoke of loving guns and combat, as well as attempting to leverage his access to classified documents to gain respect from his peers (Harwell, 2023). Teixeira was arrested on Thursday, April 13, 2023 (Dilanian, 2023).

After the documents were posted to the “Thug Shaker Central” server, they began to circulate through other Discord servers and eventually made their way onto 4chan’s political message board, /pol/. From here, the documents were spread around social media such as Twitter and Telegram (Bertrand, 2023). The documents appeared to be in the form of photos taken of physical documents, such as powerpoint slides. (Martinez, 2023).

# Impact:

## Russo-Ukrainian War:

Among the documents shared, were a large amount surrounding the ongoing Russo-Ukrainian war. These documents included casualty estimates, tactics, battle reports and more. One of the most concerning documents released detailed the current usage of Ukrainian anti-air missiles, predicting that Ukraine's air defenses would run-out by May (Cooper, 2023).

Another document released in the leak referred to 14 U.S. special operations forces as well as 97 NATO special operations forces ( Martinez, 2023).

The response to the leak’s has been varied, with U.S. discussions revolving around possible surveillance (Lee, 2023), while Ukrainian officials attempted to downplay the validity of the statements ( Martinez, 2023).

**Other Countries:**

Aside from the documents surrounding the Russo-Ukrainian war, there were many documents that related to espionage and foreign relations. Among these some of the more concerning detail information about potential Chinese involvement with Taiwan, and potential for Chinese weapons to counteract U.S. defenses there (Harris, 2023).

# Possible Preventative Measures:

The first security practice that could have helped prevent this leak would be the implementation, or improvement, of role-based privileges. However he managed to obtain physical copies of the documents, no one should be allowed to take photos of classified documents for any reason, unless expressly cleared to do so for digital storage. The fact that he was able to do this demonstrates that he had access to privileges beyond his role, and that there either need to be better policies in place to prevent this from occurring again, or existing policies need better enforcement.

Another failure demonstrated by the leak is an issue of monitoring. According to some sources, these files may have been accessible on the internet for over 2 months before the actor was found and arrested (Dilanian, 2023). This demonstrates a lack of proper logging. Given the nature of the documents, there should have been logs detailing every person who had access to, printed, or even saw the documents. This would have narrowed the search and allowed them to find the leak before it reached such a large breadth.

Due to the lack of knowledge the next point operates under the assumption that the perpetrator did not directly access the documents, but took pictures of them without permission. Under this pretense, there would need to be a clean-desk policy implemented, or the existing one enforced.

# Conclusion

These documents had a significant effect on public trust of the U.S. government, as well as public opinions on many ongoing conflicts and foreign issues. The person responsible exercised an unusual and unsafe level of privileges, violated policies and procedures, and remained anonymous for an extended period of time. In the end, proper policy and procedural enforcement, if not wholly preventing the incident, could have allowed for its quick resolution. Oversights like these are unacceptable, especially for the government of a world power.

# Works Cited

Bertrand, N., &amp; Chance, M. (2023, April 7). Pentagon investigating alleged classified

documents circulating on social media of US and NATO intelligence on Ukraine | CNN politics. CNN. Retrieved April 16, 2023, from <https://www.cnn.com/2023/04/07/politics/ukraine-documents/index.html>

Cooper, H., Barnes, J. E., Schmitt, E., &amp; Gibbons-neff, T. (2023, April 7). New Batch of

classified documents appears on social media sites. The New York Times. Retrieved April 16, 2023, from <https://www.nytimes.com/2023/04/07/us/politics/classified-documents-leak.html>

Dilanian, K., Kosnar, M., & Shabad, R. (2023, April 12). *FBI arrests 21-year-old Air*

*National Guardsman suspected of leaking classified documents*. NBCNews.com. Retrieved April 16, 2023, from <https://www.nbcnews.com/politics/national-security/us-officials-identify-leaked-classified-documents-suspect-21-year-old-rcna79577>

Harris, S., Oakford, S., & Stein, P. (2023, April 14). *Suspected leaker of top-secret*

*Pentagon documents arrested*. The Washington Post. Retrieved April 16, 2023, from <https://www.washingtonpost.com/national-security/2023/04/13/suspect-pentagon-documents-leak/>

Harwell, D. (2023, April 14). *Leak of military secrets on discord marks a new step for*

*social media*. The Washington Post. Retrieved April 16, 2023, from <https://www.washingtonpost.com/technology/2023/04/12/discord-documents-oxide-wow-mao/>

Lee, C. E., Dilanian, K., &amp; De Luce, D. (2023, April 12). U.S. may change how it monitors

the web after missing leaked documents for weeks. NBCNews.com. Retrieved April 16, 2023, from <https://www.nbcnews.com/politics/national-security/us-intel-agencies-missed-classified-documents-leaked-on-discord-rcna79404>

Martinez, L. (2023, April 9). Ukraine, North Korea and Iran included in leaked documents online.

ABC News. Retrieved April 16, 2023, from <https://abcnews.go.com/International/classified-ukraine-documents-posted-web-early-march/story?id=98433559>