Case Study: Silk Typhoon

In this age of rapidly evolving technology and processing powers, the strength of malicious cyberattacks has also evolved and has become more intricate. A cyber-attack is simply the act of gaining unauthorised access to information stored in a computer infrastructure. While cyberattacks are not necessarily malicious, such as penetration testing which is used to strengthen security, it has higher connotations to negative and harmful incidents such as the WannaCry ransomware in 2017. One recent cyberattack is the Silk Typhoon attack conducted on the US treasury in December 2024 linked to Chinese state-sponsored hackers that led to the compromise of sensitive data.

Silk Typhoon (also known as Hafnium) launched an attack on the US treasury using a stolen Remote Source SaaS API key obtained via BeyondTrust. From there, they gained access to classified documents and crucial data from the Office of Foreign Assets Control leading to a security threat in the US. This department was the only one that was affected by the data breach. Not only was BeyondTrust, a trusted vendor that works closely with the US government was affected, the unauthorised access to such crucial data at an important time in the US raised concerns around the US. BeyondTrust had to take down their services to deal with the breach in data and to also prevent further access to the treasury data. Regarding this attack, three different types of new sources covered them. One being mainstream media, the next being a more technical focused news source, while the final one is a cybersecurity focused news source. We will examine each of the three source types and compare how each source has reported on the attack.

Starting with the DarkReading news source (the cyber security focused source), we can see most of the technical information lies here. It is from here we found the main details of how the attack has occurred. By using a stolen API key and a data-theft tool known as China Chopper Web shell, they were able to override security and access the department office workstations. We also note that only Office of Foreign Assets Control was affected and anyone “can be exploited by an attacker with existing administrative privileges to inject commands and run as a site user.” It was later reported in January that BeyondTrust was able to patch up the security exploit. Despite its more technical focus on the attack, the three articles do not mention mitigation strategies other than the urging of patching a command injection flaw. The articles themselves are very concise and as such leave very little room for bias here as the main aim of the three articles is to report the information.

Following this, we will approach the technical news source (Wired). From a cursory glance, we can see that the article itself is longer than the DarkReading articles. This article more focuses on the political and aftermath of the attacks as opposed to the technical nature. While there are important technical details such as the specific vulnerabilities which were “the critical command injection vulnerability (CVE-2024-12356) and the medium-severity command injection vulnerability (CVE-2024-12686)” and what BeyondTrust is, there is not much in regards in how the attacks have occurred nor the attack vector, both of which DarkReading has reported. Aside from the FBI and BeyondTrust working to patch the vulnerability, there was no mention of mitigation strategies, which is surprising given a technology focused article. As the focus of the article was the political nature of the attack this led to bias via the use of tone, as with most political reporting. The bias was mainly towards the US government’s ill preparation in which the tone of the article followed suit.

Next, we will look at the Reuters article for the same attack, which is the mainstream media source. From even the first word, we can see it focuses more on China and how its state-sponsored hackers attacked the US Treasury. The technical information here is relegated to a single, small paragraph that uses simple descriptions so people without a cybersecurity background can understand what happened. However, the information regarding the attack vector is very broad and doesn’t give anyone with slight cybersecurity knowledge what happened or how it happened. Another notable omission is any mention of mitigation methods other than a very corporate response of taking measures. Here, we can also see that Reuters has the strongest bias of the three sources in that it fails to mention the US government’s handling of a vulnerability that, mentioned in other articles, should have been patched a while ago. Command injection vulnerabilities are usually one of the types of vulnerabilities that we look for early and prevent. Instead, it portrays China in a negative light and places the blame solely on them. As with many mainstream media, the aim is to get engagement. Therefore, painting a villain and focusing on them as opposed to the technical media accomplishes that goal for the general populace.

Comparing all 3 news sources, we can see there are some very important differences between them in terms of content and bias. DarkReading presents us with the most in-depth information about the attack vector, yet it does not tell us about what was done to mitigate/fix the attack other than pushing a fix for the command injection vulnerability. It is also noticeably smaller than the other sources, which is good in conveying technical information but does not talk about much else; it is concise. It also presents no bias due to its short length and sole focus on the cybersecurity aspect of information, which it conveys quite well but it is difficult to approach unless one has cybersecurity knowledge. On the other hand, Wired is a bit of an easier read and is noticeably longer than DarkReading . It does touch upon both technical information and the non-technical side of the arguments, but this is where bias slowly emerges despite its attempts at remaining neutral. Like DarkReading, it also does not cover the mitigation strategies, but in comparison, its technical information is a bit lacking. As it is slightly more mainstream than DarkReading, it is aiming to appeal to a wider audience as opposed to a cyber security focused source. Lastly, Reuters forgoes most technical knowledge (has little mention of how the attack occurred and has no information about mitigation efforts) and focuses on the geopolitical nature of the attack. As such, it has the most bias out of all the sources in that the article writer is biased against China. Like Wired, it aims to reach a wider audience and have greater engagement, but due to its nature as a mainstream media source, greater engagement has a higher priority, leading to stronger biases.

In conclusion, we can see that as we approach more mainstream media, we lose a fair bit of technical knowledge and gain bias due to the greater engagement requirement. This means cybersecurity attacks here are treated more broadly when reported mainstream, which can affect public perception and does not help people protect themselves from cyberattacks. Cyberattacks are also used to paint people in a negative light, so it is up to the writer/journalist to make a conscientious effort to approach it unbiasedly, but that can be difficult. On the other hand, more cybersecurity focused sources have a lot more technical depth but is inaccessible to the public. Hopefully as time progresses, reporting of these attacks can be approached unbiasedly, but it is in human nature to be biased.

Bibliography:

<https://www.darkreading.com/cyberattacks-data-breaches/hacking-group-silk-typhoon-linked-us-treasury-breach>

<https://www.darkreading.com/vulnerabilities-threats/cisa-warns-of-second-vuln-found-in-beyondtrust-breach-investigation>

<https://www.darkreading.com/cyberattacks-data-breaches/cisa-third-party-data-breach-limited-treasury-dept>

<https://www.reuters.com/technology/cybersecurity/us-treasurys-workstations-hacked-cyberattack-by-china-afp-reports-2024-12-30/>

<https://www.wired.com/story/us-treasury-hacked-by-china/>