



**NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
CYBERATTACK REPORT**

Issue Date: 11 February 2022
Designated Data Scientist: Guilherme Nogueira



This report was produced in order to provide useful information for the Government of the United States of America. It is regarding cyberattacks and its elements that threaten the National Security on a daily basis. The report was produced as a request from the Head of the National Security Agency and it is directed to him, to the President of the United States and other Bureau Agencies that might be responsible for the National Cyber Security. The raw data which this report comes from is stored at https://github.com/cyentia/sample_data_edablob/main/sample_breaches.csv.

For the analyses, cyberattacks that did not compromise any count or caused any financial impact were not considered. So far, they are considered as unsuccessful attempts. Causes qualified as “Intern” were also excluded from the analyses once it is expected that these accesses are already controled and monitored.

The sector which presented more breaches were: Financial, Professional, Healthcare, Administrative and Education (Figure 1A). There were at least 400 attacks on these sectors, and more than 700 on Financial and Professional sectors during the monitored period (2011-2020). These sectors are part of the core of the government. Maybe, this can explain why they were set as the prefferred targets. Public, Retail, Information and Manufacturing compose a second group of interest with more than 300 attacks. The remaining sectors were not represented.

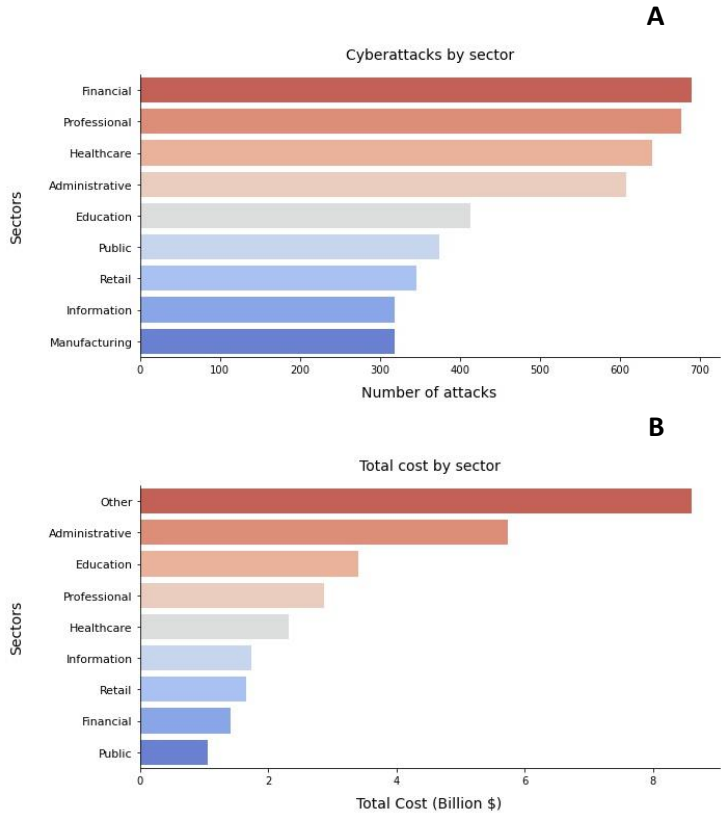


Figure 1 – Number of breaches by sector (A) and the total cost caused by breaches on each sector (B). Just the first nine sectors were considered on each graph.

However, considering the total cost that these breaches have caused, “Other” sectors stand out with an impact of more than \$8 billion dollars (Figure 1B). Further investigation on the dataset, showed that this amount comes from a single attack, occurred on 10 April 2020. More concerning than that, it is the fact the it was made by an unknown group. Although it was a single event, it caused a billionare loss for public coffers. Knowing how and where this attack occured, as so as who performed it, might prevent further attacks with such financial dimension. Aside “Other” sectors, the Administrative was the sector which breaches caused more impact with almost \$6 billion dollars as a total cost. The impact of breaches on Education, Professional and Healthcare sectors represented more than \$2 billion dollars. The impacts on Information, Retail, Financial and Public did not reach \$2 billion dollars. The remaining sectors were not represented.

Focusing the analyses on the sector that presented the highest total cost, the Administrative, it is possible to state that the Hacktivists are the most efficient groups in breaking into the Administrative sector’s system. Although it was not the group with the highest number of breaches (Figure 2A), it was the one that its breaches caused the highest total cost, more than \$2 billion dollars (Figure 2B). Criminal Organizations and Former Consultants are also important matters to consider. Their breaches caused around \$1 billion dollars of total costs.

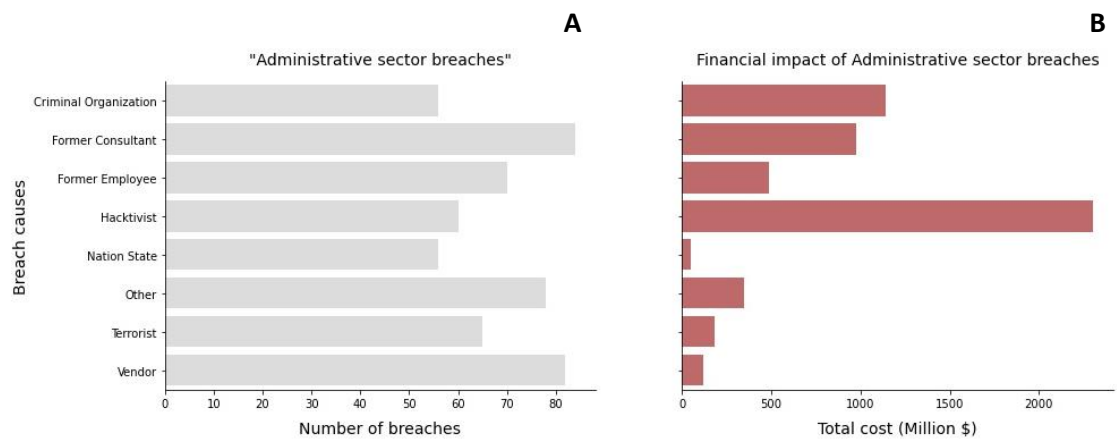


Figure 2 – Number of breaches by invading group (A) and the total cost caused by their breaches (B) on the Administrative sector

All the invading groups broke into the National System a similar number of times (Figure 3A). “Other” groups have a few more attacks, but they are not significantly different. Considering the total cost caused by each group’s breaches, “Other” groups have the highest numbers, with a total that surpasses \$10 billion dollars. However, it is important to highlight that one of these breaches was unique as presented before. Thus, for the following analyses, the 8-billion-dollar breach made by “Other” groups will not be considered in order to have a clear idea about what generally happens. Hacktivists and Former Consultants are the invading groups with the highest financial impacts (Figure 3B). Both caused breaches enough to cost more than \$4 billion dollars to the public coffers. Vendors, Criminal Organizations, Former Employees and “Other” groups, caused an impact of more than \$2 billion dollars. Nation States and Terrorists did not reach more than this amount.

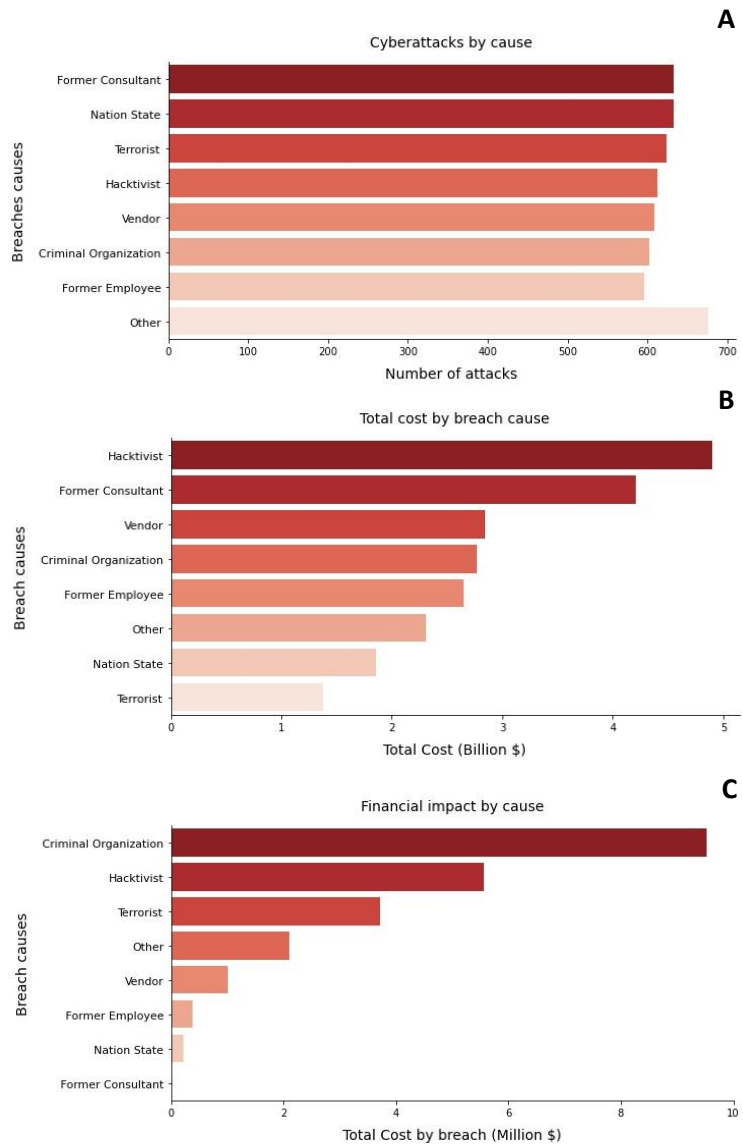
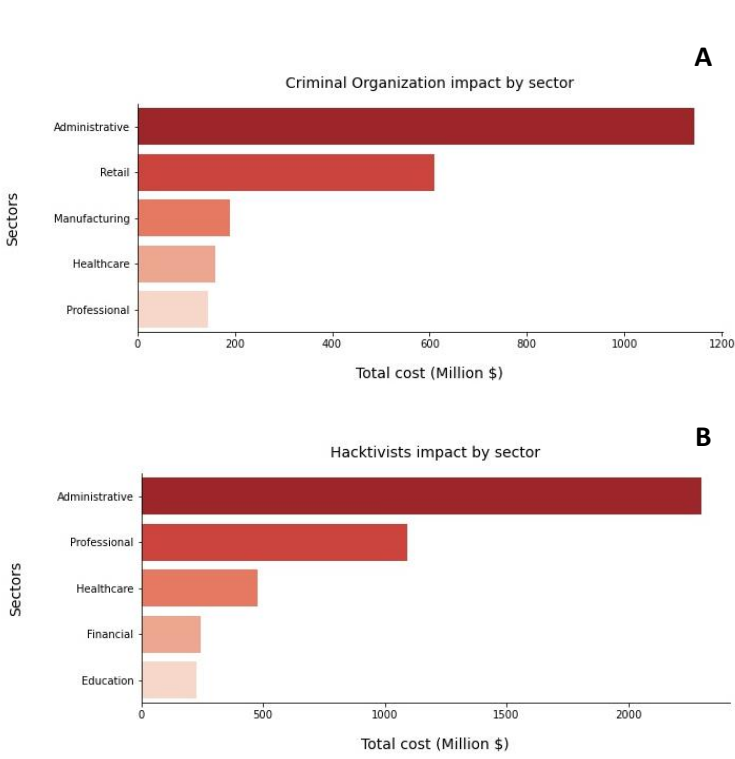


Figure 3 – Number of breaches by invading group (A) and the total cost caused by their breaches (B). Total cost by breach considering each invading group (C).

The group that causes the highest losses for the government concerning Cyber Security is the Criminal Organization (Figure 3C). They have the highest Financial Impact Rate, almost \$10 million dollars, calculated through the sum of the total costs spent on each breach divided by the total number of breaches. Basically, it represents the mean cost by breach. Hacktivists and Terrorists follow Criminal Organization with almost \$6 and \$4 million dollars of losses, respectively. “Other” groups present a lower rate, a little more than \$2 million dollars, and the remaining groups do not even reach \$ 1 million dollars by breach.

In order to have more information about Criminal Organizations and Hacktivists activities, an investigation concerning the sector(s) aimed by these groups was made. This might be really useful since it will make possible recognizing their patterns of attack. Criminal Organization groups cause more impact on the Administrative sector (Figure 4A). So far, their breaches have been causing more than \$1 billion dollars of losses. The second most impacted target concerning financial issues is the sector Retail. Criminal Organization actions caused a loss of more than \$600 million dollars. Their breaches on Manufacturing, Healthcare and Professional sectors did not cost more than \$200 million dollars, however, it is still a high amount of money. Hacktivists also cause their highest impact on the Administrative sector (Figure 4B). The total cost in this sector reaches more than \$ 2.5 billion dollars. The Professional sector reached a little more than \$1 billion dollars of costs and the sectors Healthcare, Financial and Education did not get to \$0.5 billion dollars. Only 5 sectors, which were considered the most important ones, were showed by the graphs.



Cyberattacks have been causing a high financial impact, reaching billions of dollars, and harming the resources disposed on public coffers. The Administrative sector is the one that needs more attention from the authorities. The cost that breaches have been causing on it show that something must be done in order to protect more its system. Criminal Organizations and Hacktivists are the agents that cause more losses through their breaches. It would be interesting if some lines of investigation were open to monitor and oversight their actions, leading to their further arrestment. Although it was not a pattern, the attack on “Other” sectors caused a huge financial loss in 2020. The sector in which the breach happened as well as the participants of it must be discovered as soon as possible. A window of opportunity might have been discovered, and this can lead to even higher impacts and also threaten the U.S. National Sovereignty.

Figure 4 – Criminal Organization groups (A) and Hacktivists (B) financial impact on sectors. Just the sectors with the highest impact were showed.