ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about cybersecurity incidents involving Chinese state-sponsored activities against Canadian critical national infrastructure.

Summary

Recent incidents of sophisticated cyberattacks targeting government networks in British Columbia, Canada, indicate a significant threat posed by state-sponsored actors. These attacks, suspected to be orchestrated by state actors, underscore the evolving cybersecurity landscape and the heightened risks faced by government entities. While there is no evidence of sensitive information compromise, the incidents underscore the importance of robust cybersecurity defenses. The attacks, which occurred on April 10, April 29, and May 6, involved multiple attempts to compromise government systems.

The cyberattacks coincide with recent warnings from the Canadian Security Intelligence Service (CSIS) regarding persistent interference by state-sponsored threat actors, particularly from China and India, in Canadian political affairs. The CSIS report highlights the attractiveness of Canada as a target for cyber-enabled espionage and sabotage due to its strong democratic institutions and advanced economy. Canadian authorities, including the Canadian Centre for Cyber Security and Microsoft's Detection and Response Team (DART), are actively investigating the incidents. Analysis of extensive data, totaling 40 terabytes, is underway to identify the extent of the breach and potential impacts.

David Vigneault, Director of CSIS, underscores the excellence and relevance of CSIS in fulfilling its mission to protect Canada and Canadians. He encourages all Canadians to read the newly released report to gain insights into CSIS's efforts to keep Canada safe, secure, and prosperous amidst challenging times.

Recommendations

Recommendation #1: Stay up do date

Monitor official channels to stay informed and updated on the situation involving these cybersecurity attacks.

Recommendation #2: Vigilance and monitoring

Maintain heightened vigilance and monitor network activity for suspicious behavior or indicators of compromise.

Recommendation #3: Users awareness

Educate users about cybersecurity best practices and the importance of maintaining strong passwords, identifying phishing attempts, and reporting suspicious activities.

Recommendation #4: Prepare for the Worst

ORNA **strongly recommends** that organizations ensure that all critical systems are backed up appropriately and that incident response plans are rehearsed regularly so that all participants understand their role.

References

1. The Record: https://therecord.media/british-columbia-government-canada-cybersecurity-incident
   https://therecord.media/british-columbia-government-hack-state-sponsored

2. Government of Canada: https://www.canada.ca/en/security-intelligence-service/news/2024/05/release-of-2023-public-report.html

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team