Government of Canada Summary for the Public Inquiry into Foreign Interference

PRC Email Operations Against Parliamentarians

This document has been prepared by the Government of Canada for the purpose of the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions. It responds to a specific request by the Commission for an unclassified summary of information regarding this particular topic and should not be used as the basis of understanding for any other topic. This document is based on intelligence collected and assessed over a period of time, and does not necessarily reflect to the Government of Canada's full understanding of the topic at any specific point in time. The underlying intelligence has been provided to the Commission. By employing summaries and redactions, this document sanitizes intelligence in a manner that removes the potential injury to national security and international relations, does not disclose sensitive activities, techniques, methods, and sources of intelligence that would cause potential injury, and abides by relevant Canadian legislation. It does not provide all of the caveats and limitations contained in the original classified documents or provide an assessment of the reliability or credibility of any specific piece of intelligence, as it could disclose information that could cause injury.

SUMMARY:

1. The cyber threat emanating from the People's Republic of China (PRC) is significant in volume and sophistication. The PRC uses cyber espionage techniques to collect information that will provide an economic and diplomatic advantage and frequently aims to collect large datasets containing personal information, likely for the purposes of bulk data analysis and target profiling. While Government of Canada systems have been compromised by PRC cyber threat actors multiple times over the past few years, all known compromises have been addressed.

2. As the Government of Canada's technical authority for cyber security and information assurance, the Communications Security Establishment Canada (CSE), provides advice, guidance and services to help protect the systems of federal departments and agencies, as well as other systems designated as being of importance to the Government of Canada.

3. CSE's Canadian Centre for Cyber Security (Cyber Centre) and SIGINT branches work together to meet CSE's cyber security and information assurance mandates to protect against and respond to cyber security threats facing Government of Canada infrastructure, including the House of Commons (HoC)[1]. Under its foreign intelligence mandate, CSE can collect information consistent with Canada's Intelligence Priorities to discover cyber security incidents instigated by a foreign actor and involving a Canadian victim. A formal sanitization process exists by which an UNCLASSIFIED or SECRET summary of such information can be produced to provide potential victims of cyber incidents with the necessary technical information to assess and mitigate potential threats.

4. The Cyber Centre's Incident Management team receives reports about incidents from a variety of sources, including both SIGINT and the Cyber Centre's Cyber Defence directorate. The Cyber Centre's Incident Management Operational Coordination (IMOC) team then sends unclassified

[1] It should be noted that where the House of Commons is referenced in this summary, it is a reference to the administration offices of the House of Commons, rather than a reference to the Members of Parliament.

information drawn from those reports to IT Security teams of potential victim organizations. As the systems owner, the recipient is able to then use this information to make their own assessment of the situation and to follow up with the Cyber Centre if they require further support. Organizations are not obligated to provide feedback but may enter an information exchange with the Cyber Centre to better understand the threat and potential mitigations.

5. CSE's services include the deployment, upon request (and with ministerial authorization), of network-based, cloud-based, and host-based autonomous sensors to detect malicious cyber activity on the systems it is tasked to protect. These defences block an average of 6.6 billion attempted malicious actions a day against Government of Canada networks and provide CSE with cyber threat intelligence that it shares with clients to help thwart cyber threats, including tracking link email campaigns.

6. Tracking link emails are used by cyber threat actors in an attempt to have the recipient to open an email that contains an image or other link (i.e., tracking link) that connects to a server controlled by a threat actor. This allows the threat actor to confirm the validity of the targeted email addresses and gather preliminary data about the users, such as basic device and local network information. These emails can be a precursor to follow-on activity from the threat actor.

Additional Information on malicious activity targeting parliamentary systems

7. In January 2021, CSE informed the HoC IT security officials of malicious activity targeting parliamentary systems, which were later determined to be tracking link emails targeting parliamentary email accounts.

8. From January to April 2021, CSE and the Canadian Security Intelligence Service (CSIS) met with HoC IT security officials and CSE shared at least 12 reports that contained technical indicators of compromise affecting HoC IT systems.

9. On 17 February 2021, CSE delivered a SECRET-level briefing to the HoC's IT Security officials, including the Director IT Security. CSE's brief was delivered by CSE subject matter experts with CSIS officials also in attendance. The brief focused on the threat actor designated as APT31[2]. Country, tactics and classes of targets that have historically been of interest to the threat actor, such as U.S. and Canadian politicians, were explicitly shared. At the conclusion of the brief, the HoC was invited to share threat information from their networks with the CSE/Cyber Centre that would enable the Cyber Centre to provide assistance with identifying and mitigating the malicious activity.

[2] Advanced Persistent Threat (APT) is a sophisticated cyber actor or group with the capability to conduct advanced and sustained malicious cyber activity, often with the goal of maintaining ongoing access to a victim's network. APT31 is a collection of Chinese state-sponsored intelligence officers, contract hackers, and support staff that conduct malicious cyber operations on behalf of the PRC.

10. Information reports provided by the Cyber Centre to the HoC regarding these events were subject to handling instructions indicating that information shared within the reports may only be shared with those responsible for network defence or cyber threat analysis within the intended department or organization and must be accompanied by a statement of these restrictions. Recipients are able to seek permission from CSE if they want to share information stemming from a CSE originated report, though no such requests were received. The Cyber Centre and the HoC worked together to thwart the attempted compromise by PRC cyber threat actors.

Actions following the 17 February 2021 brief

11. The 2021 APT31 cyber event highlighted three "lessons learned" within CSE regarding the response to the ongoing threat, which have directly influenced how CSE and the HoC address cyber defence issues today.

    i. Immediately following the 17 February meeting with the HoC, CSE officials internally expressed concern that the HoC had not been given sufficient information to appreciate the significance of the threat. These concerns were escalated to key executives within CSE. While the Director of IT Security for HoC was copied on most of the communication between Cyber Centre and the HoC IT Security team, more formal means of communication have since been established to improve procedures. Ultimately, this led to a renegotiation of the existing MOU between CSE and the HoC, as well as regular meetings to discuss potential incidents and services.

    ii. It was also identified that internal and overall coordination could be strengthened to ensure effective coordination between teams working on incidents such as the APT31 activity targeting the HoC. For example, a daily on-site coordination meeting on addressing threats from APT31 was implemented in late February 2021. This forum has since been replaced with the establishment of a broader National Cyber Response Unit (NCRU) in November 2021, which includes representation from, among others, the RCMP, CSIS and DND.

    iii. CSE officials also worked with HoC teams to ensure that the HoC adopted the full range of measures offered by CSE's cyber security program to better defend and respond to cyber threats. Further, an MOU between CSE and the HoC is currently being updated to better manage cyber events.

12. In November 2021, CSIS also issued a classified Analytical Brief to 35 Government of Canada clients on the topic of a tracking link campaign targeting members of the Inter-Parliamentary Alliance on China (IPAC) by PRC cyber threat actor, APT31.

13. A detailed chronology of events related to this tracking link campaign and the operational response is included at **TAB A.**