

Chronology of Events

Email Tracking Link Campaign Targeting Canadian Parliamentarians

The Communications Security Establishment Canada (CSE) has determined that cyber threat activity by the People's Republic of China (PRC) outpaces cyber threats from other nation states in volume, sophistication and breadth of targeting. The Canadian Centre for Cyber Security (Cyber Centre), a part of CSE, has observed widespread targeting by the PRC. This activity poses a serious threat to Canadian entities across a range of sectors and has targeted:

- all branches of government
- non-government organizations, academia and research institutions
- critical infrastructure
- industry, including the Canadian research and development sector

When the Cyber Centre identifies cyber threat activity targeting a Canadian or a Canadian organization, it shares this information with the system owner to assist them in identifying and mitigating the threat and notifying affected users, as required.

In January 2021, the Cyber Centre informed House of Commons (HoC) IT security officials of spear-phishing activity targeting parliamentary email accounts. These spear-phishing emails try to get the recipient to open an email that contains an embedded image (i.e., tracking link) that connects to a threat actor-controlled server. 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.

From January to April 2021, the Cyber Centre and the Canadian Security Intelligence Service (CSIS) met with HoC IT security and CSE shared at least 12 reports that contained technical indicators of compromise affecting HoC IT systems. In November 2021, CSIS issued a classified Analytical Brief to 35 GC clients on the topic of APT31's tracking link campaign targeting members of the Inter-Parliamentary Alliance on China (IPAC). In June 2022, the Federal Bureau of Investigation (FBI) released a report to CSE and CSIS detailing a PRC tracking link campaign, which included this HoC activity.


Below is the chronology of actions taken by the Cyber Centre and CSIS to notify and aid HoC officials in their detection and mitigation efforts.



Chronology of Events | Email tracking link campaign targeting Canadian parliamentarians

Note: The Cyber Centre has shared reporting related to tracking links targeting parliamentarians with the HoC and CSIS since at least late 2018.

Chronology of events

- 
- 22 January 2021** The Cyber Centre Incident Handler issues a report to the HoC IT Security Mailbox, indicating that emails containing tracking links were sent to users with @parl.gc.ca and @sen.parl.gc.ca email addresses.
- Only technical details associated with the network traffic were available.*
- 25 January 2021** The HoC Senior IT Security Analyst acknowledges receipt of the January 22 report.
- The HoC did not provide any additional feedback.*
- 29 January 2021** The Cyber Centre Incident Handler follows up with the HoC IT Security Mailbox to request feedback on the January 22 report.
- 3 February 2021** The Cyber Centre Incident Handler follows up to request feedback on January 22 report.
- The HoC Senior IT Security Analyst responded to the Cyber Centre Incident Handler and indicated that the issue was handled internally.*
- 17 February 2021** The Cyber Centre Incident Handler issues a second report to the HoC IT Security Mailbox, indicating that sophisticated actors were conducting network reconnaissance of devices known to connect to the HoC virtual private network (VPN).
- On March 1, HoC Director, IT Security, informed the Cyber Centre Incident Handler that at least one IP address was associated with the home network of an undisclosed HoC user and that the HoC was able to obtain two devices for analysis.*
- On March 5, the Cyber Centre Incident Handler made a request to HoC Director, IT Security, to perform a forensic analysis on the devices to validate that no malicious activity occurred. The HoC did not provide the devices to the Cyber Centre.*

Chronology of Events | Email tracking link campaign targeting Canadian parliamentarians

17 February
2021

HoC Director, IT Security, and representatives from CSIS and the Cyber Centre meet to discuss further collaboration on the incident.

HoC Director, IT Security, provided the Cyber Centre's Incident Management team with a printed document containing a sample malicious email and the names of eight MPs who were intended recipients of malicious emails.

According to the document, the HoC assessed at the time that the emails did not reach the intended HoC recipients. However, the HoC indicated that some recipients may have received similar messages on their personal email addresses.

18 February
2021

A Cyber Triage Unit (CTU) meeting is held between CSIS and the Cyber Centre to discuss the combined response efforts of each organization.

It was decided that CSIS would engage with the HoC. The Cyber Centre Incident Management team provided CSIS with a list of technical questions to aid in analyzing the suspicious activity.

18 February
2021

The Cyber Centre Incident Handler issues a third report to the HoC, identifying further network domain name system (DNS) traffic of concern.

19 February
2021

CSIS and the Cyber Centre meet with HoC Director, IT Security, to discuss the scope of the incident and possible forensic analysis.

22 February
2021

CSIS and the Cyber Centre meet with HoC Director, IT Security for a follow-up to the 19 February meeting.

HoC Director, IT Security, stated that the HoC team had spent a substantial amount of time looking into the incident after the 19 February meeting. HoC Director, IT Security, provided forensic data to CSIS and gave permission for Cyber Centre personnel to make a copy, which was done at the conclusion of the meeting.



Chronology of Events | Email tracking link campaign targeting Canadian parliamentarians

23 February
2021



A CTU meeting is held between CSIS and the Cyber Centre.

Following the meeting, the Cyber Centre Incident Handler provided further follow-up questions for CSIS to relay to the HoC to help with the investigation.

24 February
2021



A CTU meeting is held between CSIS and the Cyber Centre to establish a framework for joint engagements with the HoC.

Following the meeting, the Cyber Centre Incident Handler provided their investigative follow-up questions from February 23 directly to HoC Director, IT Security, and requested copies of the actual emails identified in the list. HoC Director, IT Security, did not provide the emails.

24 February
2021



The Cyber Centre Incident Handler issues a fourth report to the HoC IT Security Mailbox, indicating that sophisticated actors were scanning IP addresses that may be associated with HoC devices.

The Cyber Centre issues a fifth report to the HoC, indicating that between February 23 and 24, 2021, network DNS traffic was observed going to a previously reported domain at HoC.

26 February
2021



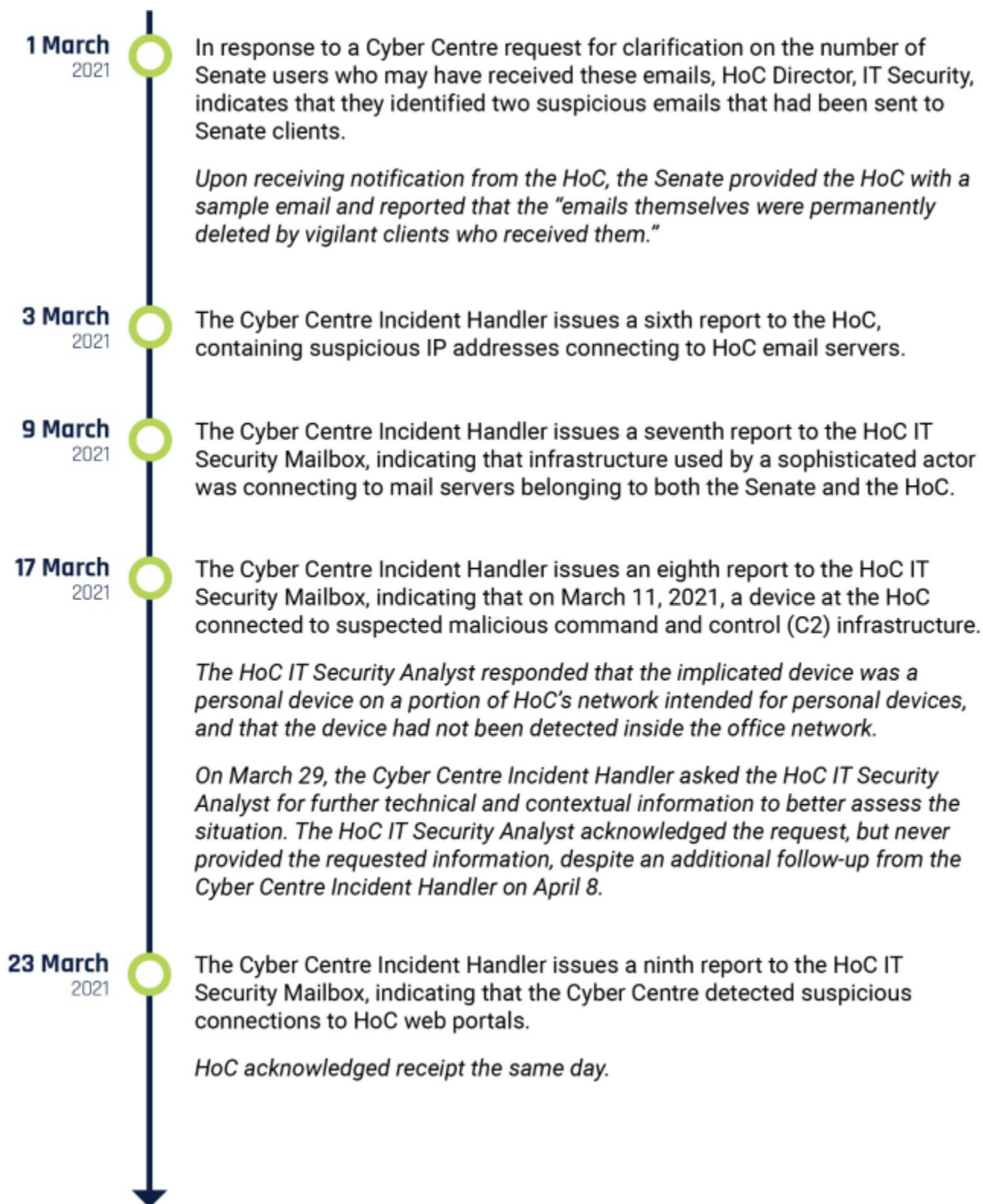
The Cyber Centre Incident Handler receives an email from HoC Director, IT Security, indicating that more emails and shared metadata for 41 emails had been sent to 13 MPs between January 21 and 28, 2021. Of those emails, 31 were either read or inadvertently opened.

Of the 13 MPs named in this email, 7 were also named in the report shared by HoC Director, IT Security, at the February 17 meeting, bringing the total number of MPs known to have received malicious emails to 14.

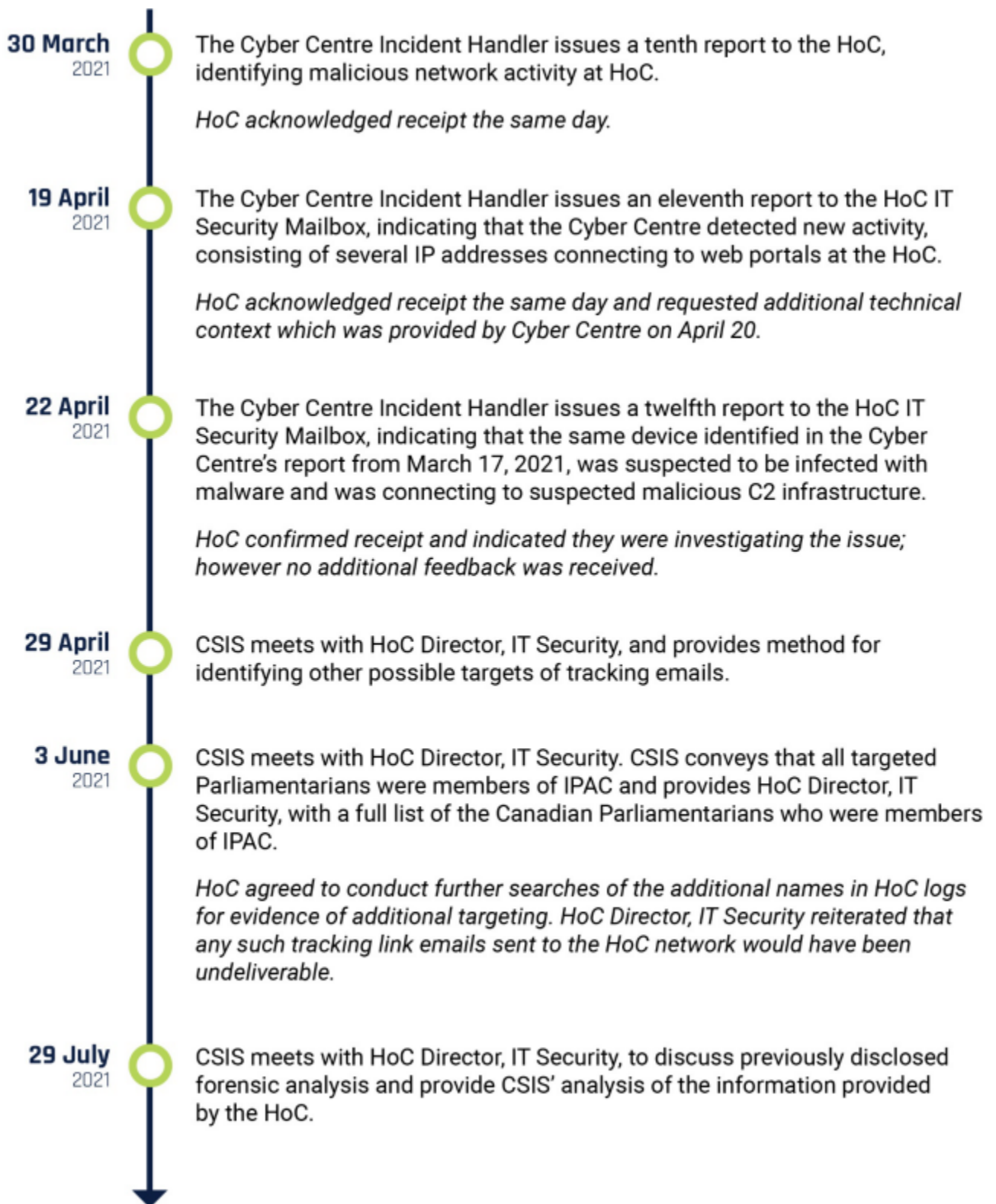
In this same email, HoC Director, IT Security, noted that, on February 10, 2021, the Senate provided information on a malicious email they received (no additional information).



Chronology of Events | Email tracking link campaign targeting Canadian parliamentarians



Chronology of Events | Email tracking link campaign targeting Canadian parliamentarians



Chronology of Events | Email tracking link campaign targeting Canadian parliamentarians

19 November
2021



CSIS issues a classified Analytical Brief to 35 GC clients on the topic of APT31's tracking link campaign targeting members of IPAC.

29 June
2022



The Cyber Centre and CSIS receive an FBI report detailing a PRC tracking link campaign, which the FBI attributed to APT31, targeting 406 unique email addresses of individuals around the world, including individuals who have been outspoken on topics relating to the activities of the Chinese Communist Party.

The report included 20 email addresses believed to have been targeted in January 2022, 19 of which were @parl.gc.ca or @sen.parl.gc.ca email addresses.

Of the 19 email addresses identified, 14 had been disclosed to the Cyber Centre by HoC Director, IT Security, on February 17, 2021 and February 26, 2021.

30 June
2022



The Cyber Centre Incident Handler shares the details of the FBI report with the HoC IT Security Mailbox, following deconfliction with CSIS.

The Cyber Centre noted that the activity was associated with a sophisticated threat actor and included a description of the techniques that had been used, the malicious indicators, the named MPs and senators, and advice on technical mitigation.

On July 4, 2022, the HoC IT Security Analyst responded to the Cyber Centre Incident Handler and indicated that the only activity they had found dated back to January 2021.

On July 21, 2022, the FBI confirmed to the Cyber Centre Incident Management Team that the activity noted in their June 2022 report had occurred in January 2021. This indicated that the FBI report described the same activity that CSIS and the Cyber Centre reported on and shared with the HoC in January 2021.

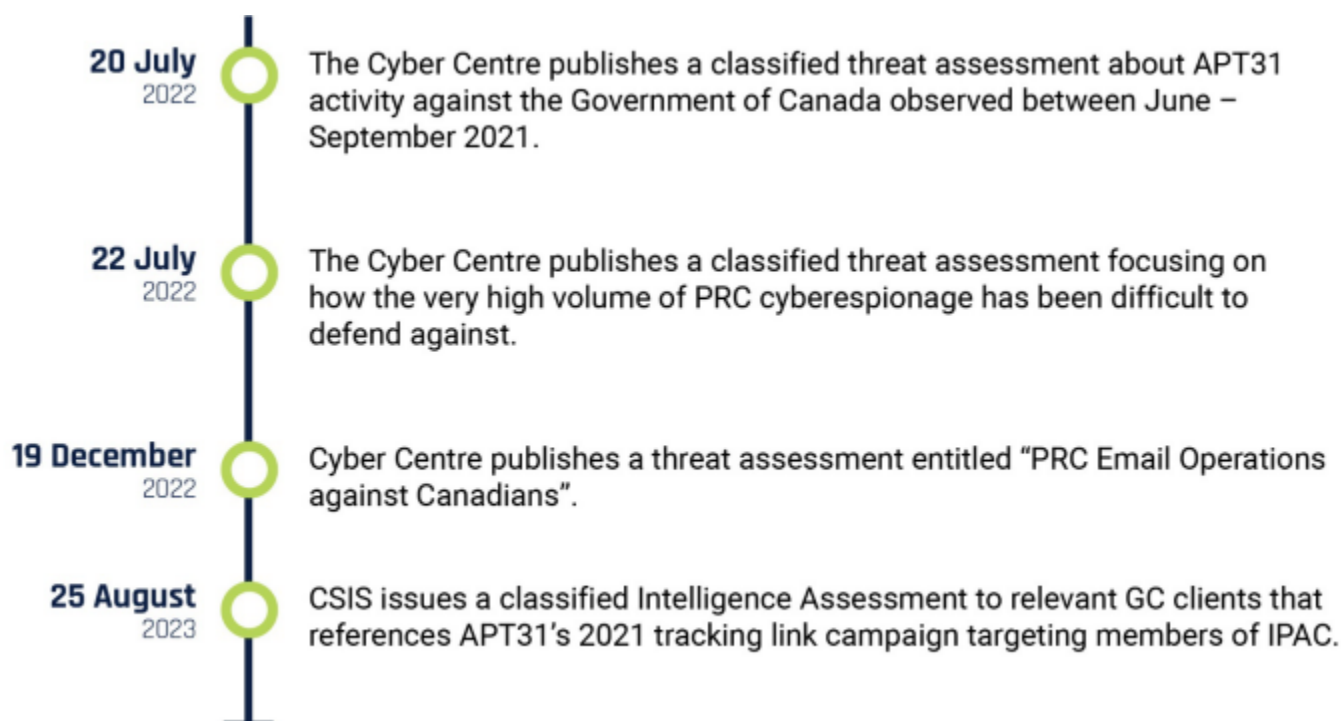
14 July
2022



The Cyber Centre publishes a classified threat assessment entitled "Revisiting PRC Email Operations against Canadian Parliamentarians".



Chronology of Events | Email tracking link campaign targeting Canadian parliamentarians



CSE Cyber Defence Tools for HoC Systems

