Canada's foreign affairs ministry hacked, some services down

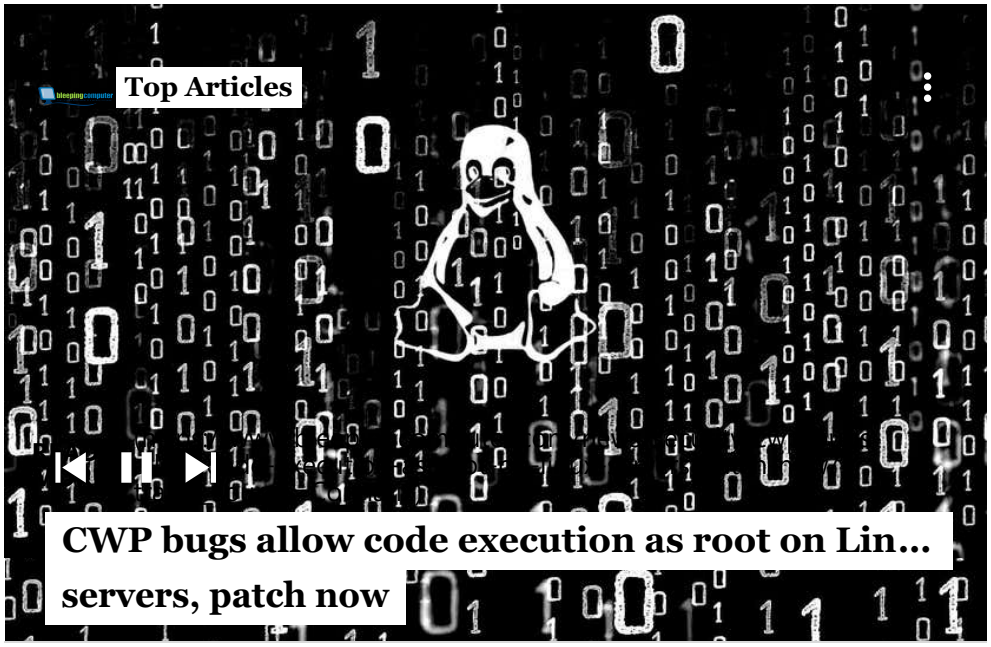
By **Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)** January 25, 2022 01:38 AM 1

The Canadian government department for foreign and consular relations, Global Affairs Canada was hit by a cyberattack last week.

While critical services remain accessible, access to some online services is currently not available, as government systems continue to recover from the attack.

Global Affairs Canada systems face network disruption

Global Affairs Canada (GAC) systems faced a network disruption after being hit with a cyberattack last week.



GAC is is the Canadian government department responsible for looking after the country's diplomatic and consular relations, international trade, and leading international development and humanitarian assistance programs.

In a statement today, Treasury Board of Canada Secretariat (TBS), Shared Services Canada, and Communications Security Establishment together confirmed (https://twitter.com/TBS_Canada/status/1485800857564336132) that a cyber incident involving Global Affairs Canada took place, sometime last week.

The attack was detected on January 19th, after which mitigation actions were taken.

The Canadian government further states while critical services continue to be available via Global Affairs' online systems, "some access to internet and internet-based services" is not available as mitigation measures have been put in place and systems undergo recovery.

There is no indication that any other government departments were impacted by the attack, explains the government.

"There are systems and tools in place to monitor, detect, and investigate potential threats, and to take active measures to address and neutralize them when they occur," says TBS.

Attack comes amid Ukraine-Russia tensions

Official sources have not yet revealed what was the cause of the attack or who are the threat actors behind it, as the investigation continues.

The cyberattack against the Canadian government comes at a time when Russia-Ukraine tensions continue to escalate.

Equally interesting is the fact that the attack happened around the same time as the Canadian Centre for Cyber Security issued a warning (https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadian-critical-infrastructure-operators-raise) to "critical infrastructure operators" to be aware of and take mitigatory actions against known Russia-backed cyber threats.

"This investigation is ongoing. We are unable to comment further on any specific details for operational reasons," says TBS.

"Our cyber defence and incident response teams work 24/7 to identify compromises and alert potential victims within the GC and Canadian critical infrastructure. The incident response team offers advice and support to contain the threat and mitigate any potential harm."

Earlier this month, multiple Ukrainian government websites were defaced (https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/), including that of the country's foreign affairs ministry.

Some suspected threat actors to be Russian although website defacement acts aren't the typical attack method used by a Russian state-sponsored hacking group like GRU (https://www.bleepingcomputer.com/news/security/us-indicts-russian-gru-sandworm-hackers-for-notpetya-worldwide-attacks/).

While the threat actors behind the incident are yet to be revealed, this isn't the first time that attackers have successfully targeted Canadian government systems.

In November 2021, the Canadian province of Newfoundland and Labrador was hit by a cyberattack causing severe disruption to healthcare providers and hospitals

(https://www.bleepingcomputer.com/news/security/canadian-province-health-care-system-disrupted-by-cyberattack/).

In early 2021, Canada Post suffered a data breach (https://www.bleepingcomputer.com/news/security/canada-post-hit-by-data-breach-after-supplier-ransomware-attack/)due to ransomware attack against one of its third-party providers

Prior to that, hackers were able to access 9,041 GCKey accounts (https://www.bleepingcomputer.com/news/security/canada-suffers-cyberattack-used-to-steal-covid-19-relief-payments/) via the "credential stuffing" technique to steal tax relief payments from Canadians.

"We are constantly reviewing measures to protect Canadians and our critical infrastructure from electronic threats, hacking, and cyber espionage," concluded the TBS, while encouraging everyone to follow cybersecurity best practices.

Related Articles:

US sanctions former Ukrainian official for helping Russian cyberspies (https://www.bleepingcomputer.com/news/security/us-sanctions-former-ukrainian-official-for-helping-russian-cyberspies/)

Multiple Ukrainian government websites hacked and defaced (https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/)

Russia arrests cybersecurity firm CEO after raiding offices (https://www.bleepingcomputer.com/news/security/russia-arrests-cybersecurity-firm-ceo-after-raiding-offices/)

Tor Project appeals Russian court's decision to block access to Tor (https://www.bleepingcomputer.com/news/security/tor-project-appeals-russian-courts-decision-to-block-access-to-tor/)

Tor’s main site blocked in Russia as censorship widens (https://www.bleepingcomputer.com/news/security/tor-s-main-site-blocked-in-russia-as-censorship-widens/)