CYBERMINUTE

Alberta Cybersecurity Insights

TLP: WHITE

Foreign Intelligence Surveillance Act (FISA)

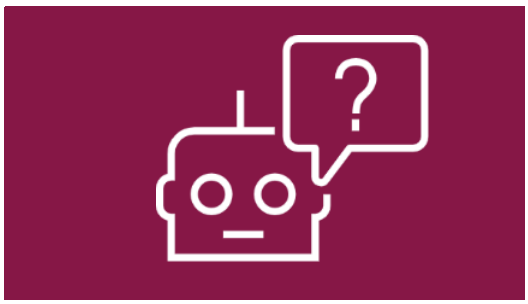
Section 702 of the Foreign Intelligence Surveillance Act (FISA) is considered a critical provision which permits the U.S. government to conduct targeted surveillance of foreign persons. In December of 2023, two competing bills were introduced which sought to amend section 702: the Protect Liberty and End Warrantless Surveillance Act (PLEWSA) and the FISA Reform and Reauthorization Act. On April 20th, 2024, President Biden signed the latter legislation—reauthorizing section 702 for two more years.

Section 702 was first established in 2008 following the post-9/11 investigations, which exposed a communications intelligence gap. At that time, the primary purpose of Section 702 was to aid in the prevention of foreign terrorist activity against the United States. It has been cited as instrumental in the thwarting of several terrorist plots. However, as technology has advanced and the threat landscape has shifted, so has Section 702. In recent years, Section 702's focus has broadened to include cyberattacks, where it has again been described as indispensable in the disruption of threats. Section 702 has led to the identification of foreign actors using U.S. infrastructure to conduct phishing attacks, it has been used to disrupt murder for hire plots, drug trafficking supply chains, to protect sensitive technology, and to combat ransomware attacks.

However, critics of Section 702 are of the view that a lack of oversight and abuse by security agencies has resulted in the unlawful and warrantless collection of U.S. persons data. These accusations are not without merit, court documents revealed that Section 702

had been misused almost 300,000 times. While Section 702 has proven its usefulness in protecting national security and safety, the privacy concerns and infringements on civil liberties cannot be ignored.

Click Here to Read More!



Large Language Model (LLM) Vulnerabilities

[On April 2nd, 2024, OpenAI competitor Anthropic disclosed a novel vulnerability that affects most of the popular Large Language Models (LLMs). When exploited, it enables users to evade the guardrails put in place by developers—a technique known as jailbreaking. This particular jailbreak exploits a feature of LLMs known as the context window, which has greatly expanded in recent years. The larger the context window, the more input an LLM can process; however, the larger this window the more vulnerable the LLM is. Anthropic highlights how "even positive, innocuous-seeming improvements to LLMs can sometimes have unforeseen consequences."

Impacts of Change Healthcare Attack

On February 21st, 2024, Change Healthcare discovered they had been the victim of a ransomware attack orchestrated by ALPHV, a notorious Russian-affiliated ransomware group. As a major payment processor in the US health sector, Change Healthcare processes 15 billion transactions annually and holds health records of one-third of U.S. residents meaning the potential scope of the attack was vast. Matching this scope, the fallout was extensive, disrupting the ability of small and midsize healthcare providers to electronically fill prescriptions and process insurance reimbursements. UnitedHealth Group, Change Healthcare's parent company, reported losses amounting to $872 million due to business interruptions.

Jailbroken models are being used by threat actors to spread misinformation and interfere with elections, improve the quality of phishing messages making them more believable, and to develop exploits. Recently, it was shown that LLMs can be used to autonomously hack websites when given access to various coding tools, data, and the internet. This increased autonomy makes LLMs more impactful and broadens their capabilities, but also transforms internal and external threats, making them more potent.

As organizations continue to adopt LLMs into their environments, it is important that they consider how they can be exploited and misused. Anthropic's discovery is a reminder of the novelty of this technology, and that as it changes, it introduces risk that is still not well understood. This is particularly concerning when one considers the breakneck pace at which this field is advancing. For these reasons, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) along with security agencies from Canada, Australia, New Zealand, and the U.K., have created a joint guidance on the secure deployment of AI systems. This guidance provides several applicable LLM specific controls, advising that organizations monitor model behaviour, perform penetration tests, and that they protect the

A week after Change Healthcare uncovered the breach, ALPHV posted proof of compromise on their leak site, alleging they had exfiltrated six terabytes of data, including information related to patients, insurance companies, pharmacies, and care providers, as well as source code used by Change Healthcare. Later in April, a second ransomware group, RansomHub, threatened to sell an additional four terabytes of Change Healthcare's data. It is believed that RansomHub is an offshoot group from ALPHV who were not paid for their work in the initial ransom and therefore targeted Change Healthcare a second time with the data they had exfiltrated in an effort to get paid.

Despite that fact that Change Healthcare paid the ransoms, experts note that there is still no guarantee that the stolen data will not appear on the dark web. Aside from the monetary impacts, there has also been severe reputational damage caused to Change Healthcare, with health providers who use the organization for payments fearing their patients' information could be leaked online, resulting in a potential glut of identity thefts, insurance fraud, blackmail, and other identity-based cybercrimes.

This incident serves as a stark reminder of the vulnerabilities in cybersecurity and the

model parameters. It is advised that organizations looking to employ these systems adhere to the security best practices described within this and similar guidance.

Click Here to Read More!

potential consequences of such attacks on critical infrastructure and sensitive data. It underscores the importance of being prepared and having a well-defined response plan to preserve operations and client data during cyber incidents. CISA does offer guidance to healthcare organizations, but this advice can be adapted for other industries. The guidance includes details on how to prepare prior to an incident, such as developing decision processes, maintaining a lists of key operational, support, and leadership contacts for use both during and after an incidents, and keeping a physical and up-to-date copy of the Standard Operating Procedure (SOP) accessible for reference during incidents.

Click Here to Read More!

CYBER ALBERTA