CYBERMINUTE

Alberta Cybersecurity Insights

TLP: WHITE

Please note that as of this CyberMinute we will be switching to a monthly cadence for this series until further notice.

RCMP Impacted by Cyber Event

On February 23, 2024, the Royal Canadian Mounted Police (RCMP) released a statement indicating that they had been the victim of a cyber attack. The details of the event are not yet known but the federal police force swiftly initiated a criminal investigation to assess the extent of what the RCMP's chief security officer is calling a cyber event.

With the incident acknowledged, an RCMP spokesperson has also clarified that there have been no operational impacts to the RCMP. Some RCMP webpages, including www.rcmp-grc.gc.ca, were non-operational as late as February 25th, although it is not clear if this was as a result of the cyber incident or if there was some other cause. This event occurred the same week as the Canadian Centre for Cyber Security released a warning urging cyber vigilance, with particular focus on preventing distributed denial of service (DDoS) attacks and webpage defacement. Some reports speculate the reason for the RCMP's webpages' downtime may be due to a DDoS attack; however, the cause of these interruptions is not yet publicly known.

In a statement given to the CBC regarding the event it was also indicated that at the time of reporting there were no known threats to Canadian's safety or security resulting from the incident. The Office of the Privacy Commissioner has also been informed about the cyber attack, ensuring that the privacy concerns of citizens are being addressed at the highest level. At time of writing, reports from the RCMP indicate that the cyber event does not appear to have affected foreign police and intelligence services either.

An RCMP spokesperson indicated that preventative measures that the organization had in place to mitigate the impact of such attacks, and the quick implementation of these measures helped prevent this from becoming a larger incident. An incident response plan, such as the one utilized by the RCMP, is a critical component of an organization's cybersecurity strategy. It provides a structured approach for handling potential threats and incidents, ensuring that the organization can respond quickly and effectively to minimize damages (e.g., prolonged system downtime, loss of sensitive data, potential regulatory fines, etc.).

Click Here to Read More!

i-Soon Leak

The recent release of i-Soon documents on a GitHub repository has provided a rare glimpse into the secretive industry that supports China's state-backed hacking efforts. It is common practice for nation state actors, like China and Russia, to contract out this nefarious work to Advanced Persistent Threats for hire. This leak indicates that i-Soon is one such contractor. Experts analyzing the leak believe that it was caused by a disgruntled employee, although this is not confirmed. Regardless, the current consensus is that the leaked documents are authentic.

Included in this leak are several custom hacking tools that have been used against foreign governments and Chinese citizens. Some highlights include:

- A X (formerly Twitter) stealer capable of obtaining user information, reading their messages, and even posting on their behalf;
- A custom Remote Access Trojan (RAT) for Windows, iOS, and Android;
- Portable equipment for attacking networks, and
- Equipment for operatives to establish secure communications.

Data leaks that provide insight into China's covert cyber operations are relatively unheard of and the tools mentioned above are only one minor component of this leak. In addition to this data, there is a trove of documents highlighting i-Soon's contracts, clients, victims, potential targets, and company dynamics. Some of the more notable insights relating to this information are as follows:

- Most of i-Soon's contracts were with the Ministry of Public Security for notably low prices;

Malware-as-a-Service InfoStealer Targeting Oil & Gas Industry

A novel phishing campaign targeting the oil and gas sector has been identified this past month. The Rhadamanthys Stealer, a type of malware-as-a-service (MaaS), is at the heart of this campaign. Rhadamanthys Stealer is a sophisticated, yet uncommon malware which can be configured to obtain sensitive information—typically credentials, cookies, sessions, or other data that can help them gain further access to a system.

The Rhadamanthys Stealer was recently updated on the black market, which may explain its sudden use in this advanced campaign. However, analysts at Cofense also note that this rise coincides with LockBit's (a well known ransomware-as-a-service group) takedown by law enforcement, potentially indicating a causal effect.

The phishing campaign uses the mask of a vehicle incident report email which has an embedded link in the message. Once this link is clicked, the following occurs:

- The link redirects the users several times, including through legitimate websites, such as Google Maps.
- The redirects lead to a domain—docptypefinder[.]info—and on this domain is an interactive PDF that contains a graphic which, if clicked, redirects to a GitHub repository.
- When redirected to that GitHub repository, a *.ZIP file is downloaded which contains a Rhadamanthys Stealer executable.
- If the user interacts with the executable, the malware unpacks and establishes a connection with a command-and-control server.

- i-Soon has compromised at least 14 foreign government agencies;
- The company was struggling financially, despite offering exceptionally low prices, indicating a large supply of these services; and
- Much of their marketing material was focused on spying capabilities, and many of their contracts were to spy on ethnic minorities and political dissidents for the government.

Although this repository of information has since been taken down by GitHub, a redacted version can still be found, and the original is easily accessible through the Way-Back Machine. Since this leak is still new, further analysis is required to determine the full extent of i-Soon's hacking efforts on behalf of China. However, to date it has shed light on the role of private contractors in supporting state-sponsored hacking activities.

Click Here to Read More!

- From here the malware exfiltrates stolen credentials, cryptocurrency wallets, and other sensitive information.

The evolution of phishing attacks through new techniques highlights the importance of ensuring users are vigilant when they engage with emails that are suspicious or from unknown senders. Training that is regularly updated to reflect modern phishing scams can go a long way to help prevent individuals from falling victim to such scams. However, an organization can also help by having good email policies in place and by blocking malicious domains—such as the docptypefinder[.]info domain cited here—to prevent users from accessing potentially malicious content.

Click Here to Read More!