CYBERMINUTE
Alberta Cybersecurity Insights

TLP: WHITE

Preliminary Lessons Learned: Clearview Resources Ltd. Cyber Incident

In early December 2023, Clearview Resources Ltd. disclosed that they had been impacted by a cyber incident. At the time, the Calgary-based energy producer acknowledged the incident but held back further comment until an initial investigation had been completed. On January 12, 2024, Clearview provided an update based on the preliminary investigation. In the update, the company stated that the incident was due to a compromised internal email address, which was used by the cybercriminals to transfer $1.5 million of company funds to an unsanctioned account, likely controlled by the threat actor.

Also discussed in their statement were the steps that Clearview took in response to the incident, which included working with their IT service provider to disable unspecified IT functions with no appreciable impact to the organization's operations. Clearview is continuing to investigate the incident and work towards recovering the lost funds. However, when it became clear that the threat actors did not pose any further risk to the company's systems, the previously disabled IT functions were restored.

While it is not 100% clear from their statement, it is likely that business email compromise was the impetus of the incident experienced by Clearview. Business email compromise is a common type of spear phishing where the email address of a trusted party (e.g., internal business email, third-party vendor, etc.) is compromised or spoofed to lend validity to a monetary or information request. According to the RCMP website, it is "one of the most financially damaging online crimes."

To prevent such incidents, it is suggested that organizations prioritize employee training and employ comprehensive procedures for handling potentially sensitive requests (e.g., requests for payment, information requests, etc.). Regular security audits are also recommended to assess the effectiveness of the organization's cybersecurity practices and controls. With responses to cyber incidents likely becoming more and more regulated, as various levels of government begin to discuss repercussions for failure to adequately protect against a cyber incident, regular audits will become more important in ensuring an organization is compliant not only with internal controls but regulations and laws. Several organizations, such as the City of St. Albert, have already announced such audits for 2024, highlighting a positive shift not only in completing these audits but a willingness to discuss and bring awareness to the importance of cybersecurity.

Click Here to Read More!

The Threats of AI to the Democratic Process

Attempts by nation state threat actors—often China, Russia, and Iran—to sway elections by influencing voter opinion, or to inflict chaos and confusion are not novel. The motivation behind these attacks has remained consistent; however, with the technological advancements such as those in Artificial Intelligence (AI), these attacks are becoming increasingly sophisticated and numerous. This revelation has resulted in officials—such as the director of the Federal Bureau of Investigations (FBI), the National Security Agency (NSA), and the head of Canadian Center for Cybersecurity (CCCS)—to issue concerns. These concerns are compounded by the upcoming 2024 election cycle(s), said to be the largest spate of elections in history with at least 64 participating countries.

AI Generators are being increasingly weaponized in the spread of disinformation, a trend that was outlined in the CCCS's 2023, Cyber Threats to Canadas's Democratic Process report. Below is a list of only a few of these generators, all of which are publicly available:

- **ChatGPT** is free and can produce text that is indiscernible from text generated by humans. This can be used by threat actors to produce convincing misinformation campaigns.
- **DALLE-2** can generate realistic images which can be used to slander, "stir the pot", or create believable profile pictures for use by social media bots.
- **HeyGen** can be used to generate deep fakes, and has been implicated in the spread of misinformation on sites like Meta (Facebook) for the purpose of disrupting Bangladesh's election.
- **Speechify** allows users to clone voices after being provided a short recording.

X Accounts Targeted for Crypto Scams

Since the beginning of the year, there have been several hacks of high-profile X (formerly Twitter) accounts. The targets of these attacks have been individuals or organizations that have gold or grey checkmarks on their X accounts. A gold checkmark indicates that the account has been validated as belonging to an official organization, while the grey checkmark indicates that the account belongs to a government entity or official. These accounts are becoming popular targets for hacking because of the trustworthiness implicit with them, as the accounts have been through a rigorous validation process. This means that cybercriminals that take over such accounts are more likely to have their posts believed, due to the trust created by the checkmarks, making them useful in phishing and digital fraud attempts.

A few accounts that have been targeted include Canadian Senator Amina Gerba, the cybersecurity company Mandiant, the US Security and Exchange Commission, and the municipality of Peterborough in Ontario, to name but a few. Of the examples listed, it is noteworthy that all of them were used to promote cryptocurrency scams. According to experts, this is due to a rise in drainers-as-a-service platforms, which provide crypto drainers (malware that redirects funds from a victims crypto wallet) that can be linked to in hacked messages. When combined with the perceived trust in verified accounts this can result in many more people being scammed.

In light of these hacks the importance of enabling multi-factor authentication (MFA) has been raised, as both Mandiant's and the Security and Exchange Commission's accounts did not have MFA activated, likely facilitating the hack. At time of writing, neither Gerba nor Peterborough have stated whether MFA was enabled on their accounts when they were hacked. In response to

Threat actors can use this to slander opponents, by “making them say” egregious things.

The age of authenticating a campaign message by appending it with a recorded approval has ended. Furthermore, attempts to identify AI generated material have proven to be an intractable problem. Currently, the prescribed antidote is awareness and a critical eye. Additionally, the NSA has identified the defense of AI models as critical to national security. However, the damage may already be done, as noted by the director of the FBI, attempts to undermine the electoral process—successful or not—are enough to diminish confidence in the democratic process.

Click Here to Read More!

criticism about hacked accounts, X responded with recommendations for protecting X accounts, including enabling MFA, using strong passwords, requiring email or phone confirmation for changing passwords, and general cyber hygiene such as suspicion of links and not sharing credentials.

Click Here to Read More!