CYBERMINUTE
Alberta Cybersecurity Insights
Alberta

TLP: WHITE

Government of Canada Seeking to Ban the Flipper Zero Hacking Device

On February 8th, Public Safety Canada issued a statement of intent regarding the auto theft epidemic in Canada. An estimated 90,000 vehicles are stolen annually, which equates to approximately $1 billion in annual losses. In the federal action on combatting auto theft, the Innovation, Science and Economic Development institution of Canada stated their intent to ban the sale of devices used to steal vehicles; specifically naming the Flipper Zero. This would contribute to the removal of the Flipper Zero and similar portable hacking devices—e.g., HackRF one—from the Canadian marketplace. Notably, the use of rolling codes since the 1990s means that the Flipper Zero can only directly target cars made prior to this date.

The Flipper Zero is a Swiss army knife for penetration testers, empowering users to interact with and manipulate a multitude of systems. It can read, write, store, and emulate low and high frequency data to overcome basic access control systems. For example, an attacker using the Flipper Zero can record the signal a garage door remote uses to open said door, store that signal, then replay it later. This is referred to as a replay attack, and it enables the Flipper Zero to imitate the target device.

The intent of the Canadian government highlights the impact that tools such as the Flipper Zero can have in the hands of organized and motivated criminals. But such tools also have positive impacts which would be negated by this ban. Researchers can use the Flipper Zero to identify and disclose vulnerabilities in systems and devices such as key fobs. This can subsequently lead to the production of securer devices, and much needed security patches. Whether this ban will go through or be an effective countermeasure against car theft is still unclear; however, it draws awareness to yet another way individuals can be targeted by cybercriminals.

Click Here to Read More!

$25 Million Lost in Deepfake Fraud Attack

In early February, an organization in Hong Kong allegedly suffered a $200 million HKD—approximately $34.5 million CAD—loss due to a sophisticated fraud attack. While the crime started with an email—later confirmed to be a compromised account—requesting confidentiality on a large transaction, the noteworthy element was what happened next. The cybercriminals used a generative video AI technology—also referred to as a deepfake video—to impersonate the company's chief financial officer during a staged video conference. While the attack is still under investigation, it looks set to mark a turning point in the evolution of social engineering attacks.

It is heavily suspected by TrendMicro analysts that this attack utilized commercial AI tools to create the deepfaked video used during the call. This technology is constantly evolving, but from a few minutes of video of the real individual these tools can be used to create a new clip where the AI creates a video of the person following a script provided by the client—in this case a cybercriminal. This incident highlights the increasing influence of AI in cybercrime, particularly in social engineering and fraud related crimes. It also underlines the possibly expanded cost the marrying of AI and cybercrime.

Business email compromise, as seen in this incident, is often considered one of the most profitable cyberattack methods and the use of AI is making it more compelling and effective. This means it is critical for organizations to have steps in place to make them resistant to fraud. This can include employee training, keeping abreast of novel threats, and ensuring email filtering policies are kept up-to-date. The incident also underscores the importance of having a clearly defined verification process for the transfer of funds; a process that is upheld regardless of who is requesting the transfer, adopting the “never trust, always verify” mantra of zero-trust frameworks.

Click Here to Read More!

Five Years ‘Living Off the Land’: Volt Typhoon

According to a joint statement released on February 7, 2024 by American intelligence and allied agencies from Australia, Britain, Canada, and New Zealand, a sophisticated group of hackers, known as Volt Typhoon (a.k.a. Bronze Silhouette, Insidious Taurus), has been actively targeting US critical infrastructure for as long as five years. The Chinese-based group is reported to have infiltrated various sectors including companies in the transportation, oil and utilities, communication, and water sectors, although specific organizations who were targeted have not been publicly disclosed.

Volt Typhoon is known for using living off the land techniques in their attacks on critical infrastructure organizations. Unlike many groups that utilize these techniques, Volt Typhoon does not focus their attacks on espionage, preferring attacks which result in destruction or disruption. While the group shies away from collecting information from the organizations they attack, they do conduct extensive reconnaissance beforehand about the company. This allows them to create bespoke tactics, techniques, and procedures (TTPs) when targeting the victim company, customizing them to match the organization’s environment, often lengthening the time it takes for the infiltration to be discovered. This being said, in the aforementioned statement, CISA did release some of the observed TTPs used by the group.

The widespread nature of the hacks has led to meetings between the White House and private industry, with the US government seeking assistance in tracking Volt Typhoon’s activity. The American government has reportedly launched an operation to combat the group by remotely disabling aspects of its operations.

Activities organizations can take to mitigate against Volt Typhoon activity according CISA include:

- Keeping up to date on patches and updates for internet facing systems, with priority given to mitigating critical vulnerabilities that are known to be exploited by the group.

- Utilizing multi-factor authentication wherever possible, avoiding authentication methods prone to phishing (e.g., SMS, email).
- Enabling application, access, and security logs (at a minimum).
- Storing logs in a centralized system.

Currently in Canada, Bill C-26 is being debated in parliament and, if passed, would force organizations who are members of critical infrastructure sectors to strengthen their cybersecurity. The Bill is being considered in an effort to mitigate against attacks from groups like Volt Typhoon by ensuring companies in critical sectors meet a certain baseline of cybersecurity.

Click Here to Read More!

© Cybersecurity Division 2024