
## September 20, 2022

**Challenge yourself with our Ransomware Quiz!**

This past week's stories:

- **Canada targeted by dozens of cyberespionage attacks since 2010, study shows**
- **Police warn public in regards to callback phishing scams**
- **Uber names hacking group responsible for cyberattack**
- **Grand Theft Auto VI footage leaked after hack, developer Rockstar confirms**
- **China looks to increase penalties under its cybersecurity law**
- **New York ambulance service discloses data breach after ransomware attack**
- **Revolut hit by data breach, users warned of phishing attacks**
- **American Airlines admits data breach**
- **LastPass reveals hackers had access to its system for four days**
- **Alert issued over cybersecurity concerns in hundreds of medical devices**
- **Hacker steals $160 million from crypto trading firm Wintermute**
- **Cyberattack costs for US businesses up by 80%**

---

### Canada targeted by dozens of cyberespionage attacks since 2010, study shows

A new academic analysis has identified at least 75 foreign digital operations of a malicious political or industrial nature directed at Canada since 2010 — from attempts to steal COVID-19-related research to the targeting of Uyghur human rights activists.

The report by researchers at the University of Quebec at Montreal's Observatoire des conflits multidimensionnels found cyberespionage accounted for more than half of these episodes.

https://globalnews.ca/news/9130927/canada-cyber-spying-threats-study/

*Click above link to read more.*

Back to top

## Police warn public in regards to callback phishing scams

While making a phone call may seem harmless, you should always consider who's on the other end of the line. Cybercriminals can use callback phishing scams to trick you into calling them directly. Once you're on the phone, cybercriminals will ask you to share sensitive information or grant them access to your device.

In one scam, cybercriminals send you an email that says you've subscribed to a service with automatic payments. The email also includes a phone number that you can call if you have any questions. When you call the phone number, the cybercriminals will ask for remote access to your desktop so that they can cancel the subscription for you.

https://www.kingstonpolice.ca/en/news/police-warn-public-in-regards-to-callback-phishing-scams.aspx

*Click above link to read more.*

Back to top

---

## Uber names hacking group responsible for cyberattack

Uber's computer network was breached by a cyberattacker last Thursday, who Uber now says hacked into the account of an EXT contractor after likely purchasing the employee's credentials from the dark web. In a blog post Monday, Uber said it is likely the contractor's personal device had been infected with malware, leading to those credentials becoming exposed.

Though Uber has online safety precautions in place for employee logins, the contractor unknowingly accepted a verification notification that ultimately granted the attacker access, the ride-share company said. From there, the attacker accessed several employee accounts and tools such as G-Suite and Slack.

https://www.cnet.com/tech/services-and-software/uber-reports-hacking-group-responsible-for-cyber-attack-lapsus/

*Click above link to read more.*

Back to top

---

## Grand Theft Auto VI footage leaked after hack, developer Rockstar confirms

More than 90 videos and images from the next edition of the Grand Theft Auto franchise have been leaked online by a hacker, the game's developers say.

The leaked content was posted on Sunday after what is being described as one of gaming's biggest security breaches.

https://www.bbc.com/news/technology-62960828

*Click above link to read more.*

Back to top

---

## China looks to increase penalties under its cybersecurity law

China's cyberspace regulator on Wednesday proposed a series of amendments to the country's cybersecurity law including raising the size of fines for some violations, saying that it wanted to do so to improve coordination with other new laws.

The Cyberspace Administration of China (CAC) said, for example, that it wanted to introduce a penalty that would see operators of critical information infrastructure which used products or services that had not undergone security reviews be fined up to an equivalent of 5% of their previous year's revenue, or 10 times the amount they paid for the product.

https://www.reuters.com/world/china/china-seeks-public-comment-possible-amendments-cybersecurity-law-2022-09-14/

*Click above link to read more.*

Back to top

---

## New York ambulance service discloses data breach after ransomware attack

Empress EMS (Emergency Medical Services), a New York-based emergency response and ambulance service provider, has disclosed a data breach that exposed customer information.

According to the notification, the company suffered a ransomware attack on July 14, 2022.

An investigation into the incident revealed that the intruder had gained access to Empress EMS' systems on May 26, 2022. About a month and a half later, on July 13, the hackers exfiltrated "a small subset of files," a day before deploying the encryption.

https://www.bleepingcomputer.com/news/security/new-york-ambulance-service-discloses-data-breach-after-ransomware-attack/
*Click above link to read more.*

Back to top

---

### Revolut hit by data breach, users warned of phishing attacks

Financial technology firm Revolut has suffered a cyberattack that saw sensitive client information accessed by threat actors.

The company has confirmed the “highly targeted" attack, which saw hackers gain access to internal systems through phishing, rather than malware(opens in new tab) or viruses. The access lasted “for a short period of time” during which the details of 0.16% of Revolut’s customers were reportedly accessed.

https://www.techradar.com/news/revolut-hit-by-data-breach-users-warned-of-phishing-attacks

*Click above link to read more.*

Back to top

---

### American Airlines admits data breach

American Airlines experienced a breach of its customer and employee data in early July. The company announced the hack more than two months later in a letter to affected customers sent on Friday, and first shared as a PDF by Bleeping Computer.

“The personal information involved in this incident may have included your name, date of birth, mailing address, phone number, email address, driver’s license number, passport number, and/or certain medical information you provided,” the airline wrote to customers. Though, the company claimed to have “no evidence” that customers’ personal information has been misused.

https://gizmodo.com/american-airlines-data-breach-travel-flights-1849557150

*Click above link to read more.*

Back to top

---

### LastPass reveals hackers had access to its system for four days

LastPass, a password management company, has revealed details of the security incident that occurred last month in its development environment, which resulted in the theft of a portion of its source code and technical information.

It emerged that the threat actor had been given access to LastPass' systems for four days but could not obtain sensitive customer information due to the system design and the zero-trust controls put in place to prevent such incidents.

https://www.itworldcanada.com/post/lastpass-reveals-hackers-had-access-to-its-system-for-four-days

*Click above link to read more.*

Back to top

---

### Alert issued over cybersecurity concerns in hundreds of medical devices

In the U.S., the FBI has found hundreds of vulnerabilities in medical devices following recent Cybersecurity and Infrastructure Security Agency (CISA) alerts. These medical devices, including insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers and intrathecal pain pumps, all too often run outdated software and lack adequate security features.

As an example, the CISA has called out vulnerabilities in the Contec Health CMS8000 Vital Signs Patient Monitor. This is a device that's designed to monitor a patient's heart rate, oxygen saturation, temperature, and other vital signs.

https://www.digitaljournal.com/tech-science/alert-issued-over-cybersecurity-concerns-in-hundreds-of-medical-devices/article

*Click above link to read more.*

Back to top

---

### Hacker steals $160 million from crypto trading firm Wintermute

In the latest eye-watering crypto heist, Wintermute, a market-making firm, has been hacked for $160 million, according to its CEO.

Early Tuesday morning, CEO Evgeny Gaevoy posted on Twitter that the company was experiencing an ongoing hack that had drained the funds from its decentralized finance (DeFi) operations.

https://www.theverge.com/2022/9/20/23362864/hacker-crypto-steal-wintermute-theft

*Click above link to read more.*

Back to top

---

### Cyberattack costs for US businesses up by 80%

In seven out of eight countries, cyberattacks are now seen as the biggest risk to business — outranking COVID-19, economic turmoil, skills shortages, and other issues. The "Hiscox Cyber Readiness Report 2022," which assesses how prepared businesses are to fight back against cyber incidents and breaches, polled more than 5,000 corporate cybersecurity professionals in the US, UK, Belgium, France, Germany, Ireland, Spain, and the Netherlands. These experts had some enlightening things to say.

Cyberattacks Are a Bigger Concern for US Businesses Than the "Great Reshuffle"

According to the report, IT pros in US businesses are more worried about cyberattacks (46%) than the pandemic (43%) or skills shortages (38%). And the data prove it. The survey indicates that in the past 12 months, US businesses weathered a 7% increase in cyberattacks. Approximately half of all US businesses (47%) suffered an attack in the past year.

https://www.darkreading.com/attacks-breaches/cyberattack-costs-for-us-businesses-up-by-80-

*Click above link to read more.*

Back to top

---

**Click unsubscribe to stop receiving the Digest.**

**********



For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer