
## May 23, 2023

**Challenge yourself with our Vulnerability Management Quiz!**

This past week's stories:

- **Data breach of SINs at one of Canada's largest investment firms 'so dangerous'**
- **New ZIP domains spark debate among cybersecurity experts**
- **US offering $10m reward for Russian man charged with ransomware attacks**
- **Clinic goes offline after alleged cyber security attack**
- **ScanSource ransomware attack: 5 big things to know**
- **Experts say that AI has made hacking your password easier**
- **Time taken for hackers to crack passwords revealed**
- **Nozomi introduces AI cybersecurity engine to protect critical infrastructure**
- **NextGen Healthcare data breach leaks 1 million patient records, including social security numbers**
- **3 ways hackers use ChatGPT to cause security headaches**
- **Dorchester school IT system held to ransom in cyber attack**
- **Dish says ransomware gang stole almost 300,000 employee records**

---

### Data breach of SINs at one of Canada's largest investment firms 'so dangerous'

A data breach of social insurance numbers (SIN) belonging to the clientele of one of Canada's largest investment firms is "so dangerous," according to a former high-level employee at the company.

https://toronto.ctvnews.ca/data-breach-of-sins-at-one-of-canada-s-largest-investment-firms-so-dangerous-1.6402642

*Click above link to read more.*

Back to top

---

### New ZIP domains spark debate among cybersecurity experts

Cybersecurity researchers and IT admins have raised concerns over Google's new ZIP and MOV Internet domains, warning that threat actors could use them for phishing attacks and malware delivery.

https://www.bleepingcomputer.com/news/security/new-zip-domains-spark-debate-among-cybersecurity-experts/

*Click above link to read more.*

Back to top

---

### US offering $10m reward for Russian man charged with ransomware attacks

Mikhail Pavlovich Matveev, a 30-year-old Russian national, has been charged by the US Justice Department for his alleged role in numerous ransomware attacks, including ones targeting critical infrastructure.

https://www.securityweek.com/us-offering-10m-reward-for-russian-man-charged-with-ransomware-attacks/

*Click above link to read more.*

Back to top

---

### Clinic goes offline after alleged cyber security attack

Patients have been lining up outside of a local allergy, asthma and immunology clinic for much needed injections, while the clinic tries to recover from what they said is a cyber security breach.

https://kfor.com/news/local/clinic-goes-offline-after-alleged-cyber-security-attack/

*Click above link to read more.*

Back to top

---

### ScanSource ransomware attack: 5 big things to know

Amid what some cyberthreat experts are saying is a resurgence in ransomware overall in 2023, IT and telecom distributor ScanSource confirmed this week it has become the victim of what appears to be a major ransomware attack. The cyberattack has crippled some of ScanSource's basic digital systems, including many pages on its website, impacting customers and suppliers in geographies including North America, according to the Greenville, S.C.-based company.

https://www.crn.com/news/security/scansource-ransomware-attack-5-big-things-to-know

*Click above link to read more.*

Back to top

---

### Experts say that AI has made hacking your password easier

A survey of Cyber Security experts has found that since the birth of conversational Artificial Intelligence-powered chatbots, there is a higher-level threat of hackers stealing credentials and phishing for sensitive information.

https://tech.co/news/experts-agree-ai-hacking-easier

*Click above link to read more.*

Back to top

---

### Time taken for hackers to crack passwords revealed

New Specops Software research has unearthed the length of time it takes modern attackers to brute force user passwords. Plain text password storage is rare in these modern times, requiring attackers to adopt password cracking methods to make use of the majority of (hashed) password leaks. However, with the help of newer password-cracking hardware and software, the time to crack passwords is now considerably short.

https://www.itsecurityguru.org/2023/05/18/time-taken-for-hackers-to-crack-passwords-revealed/

*Click above link to read more.*

Back to top

---

### Nozomi introduces AI cybersecurity engine to protect critical infrastructure

IoT security solutions firm Nozomi has announced the launch of Vantage IQ, an AI-based analysis and response engine designed to address security gaps and resource limitations in critical operational infrastructure.

https://www.telecomstechnews.com/news/2023/may/18/nozomi-ai-cybersecurity-engine-protect-critical-infrastructure/

*Click above link to read more.*

Back to top

---

### NextGen Healthcare data breach leaks 1 million patient records, including social security numbers

A data breach on the U.S. healthcare software giant NextGen Healthcare Inc. has exposed over 1 million patient records.

https://www.cpomagazine.com/cyber-security/nextgen-healthcare-data-breach-leaks-1-million-patient-records-including-social-security-numbers/

*Click above link to read more.*

Back to top

---

### 3 ways hackers use ChatGPT to cause security headaches

With ChatGPT making headlines everywhere, it feels like the world has entered a Black Mirror episode. While some argue artificial intelligence will be the ultimate solution to our biggest cybersecurity issues, others say it will introduce a whole slew of new challenges.

https://www.darkreading.com/vulnerabilities-threats/3-ways-hackers-use-chatgpt-to-cause-security-headaches

*Click above link to read more.*

Back to top

---

### Dorchester school IT system held to ransom in cyber attack

A school has been left unable to use email or accept payments following a cyber attack.

https://www.bbc.com/news/uk-england-dorset-65685607

*Click above link to read more.*

Back to top

---

### Dish says ransomware gang stole almost 300,000 employee records

U.S. satellite television giant Dish has confirmed that hackers stole the personal information of almost 300,000 individuals during a February ransomware attack.

https://techcrunch.com/2023/05/22/dish-says-ransomware-gang-stole-almost-300000-employee-records/

*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