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

## January 18, 2022

**Challenge yourself with our Cyber Security Resolutions quiz!**

This past week's stories:

🍁 **Timmins company certified in cyber security**

🍁 **Employee information may have been accessed in cyber attack: SLGA**

🍁 **B.C. man loses retirement savings to cryptocurrency scam**

**REvil ransomware gang arrested in Russia**

**Largest darknet stolen credit card site closes**

**Critical Cisco contact center bug threatens customer-service havoc**

**Microsoft RDP bug enables data theft, smart-card hijacking**

**High-severity vulnerability in 3 WordPress plugins affected 84,000 websites**

**AWS Glue flaw let attackers access AWS customer accounts**

**DHL dethrones Microsoft as most imitated brand in phishing attacks**

**How a hacker controlled dozens of Teslas using a flaw in third-party app**

**7 strategies to improve cybersecurity in 2022**

**Cyberattacks surge amid accelerating pace of Covid-driven digitalisation: WEF study**

---

### Timmins company certified in cyber security

A Timmins company is the first in Northern Ontario to achieve "cybersecure status" under a nationally recognized program.

Timmins Mechanical Solutions has received its CyberSecure Canada certification, one of only 20 companies in the country to do so.

An initiative of the federal government, the certification process recognizes small and medium organizations that have put into place cyber-secure systems and risk management protocols in order to keep their online activities secure.

https://www.timminstoday.com/local-business/timmins-company-certified-in-cyber-security-4961786

*Click above link to read more.*

Back to top

---

### Employee information may have been accessed in cyber attack: SLGA

Some personal information of Saskatchewan Liquor and Gaming Authority (SLGA) employees may have been accessed during a cyber attack on Dec. 25, the Crown reported Monday.

In a news release, SLGA said based on the findings of its ongoing investigation into the "cyber security incident," there is a risk that personal information may have been accessed by a third party.

https://regina.ctvnews.ca/employee-information-may-have-been-accessed-in-cyber-attack-slga-1.5743484

*Click above link to read more.*

Back to top

---

### B.C. man loses retirement savings to cryptocurrency scam

The Canadian Anti-Fraud Centre says there has been a 5,600% increase in cryptocurrency fraud since 2015 and a B.C. man who lost his retirement savings is among the victims. Consumer Matters reporter Anne Drewa has this cautionary tale.

https://globalnews.ca/video/8518726/b-c-man-loses-retirement-savings-to-cryptocurrency-scam

*Click to watch the video*

Back to top

---

### REvil ransomware gang arrested in Russia

Authorities in Russia say they have dismantled the ransomware crime group REvil and charged several of its members.

The United States had offered a reward of up to $10m (£7.3m) for information leading to the gang members, following ransomware attacks.

https://www.bbc.com/news/technology-59998925

*Click above link to read more.*

Back to top

---

### Largest darknet stolen credit card site closes

The administrators of the largest illegal marketplace on the darknet for stolen credit cards are retiring after making an estimated $358m (£260m).

The anonymous owners of UniCC thanked the criminal fraternity for their business, citing age and health for the closure.

https://www.bbc.com/news/technology-59983950

*Click above link to read more.*

Back to top

---

### Critical Cisco contact center bug threatens customer-service havoc

Attackers could access and modify agent resources, telephone queues and other customer-service systems – and access personal information on companies' customers.

A critical security bug affecting Cisco's Unified Contact Center Enterprise (UCCE) portfolio could allow privilege-escalation and platform takeover.

https://threatpost.com/critical-cisco-contact-center-bug/177681/

*Click above link to read more.*

Back to top

---

### Microsoft RDP bug enables data theft, smart-card hijacking

Microsoft Windows systems going back to at least Windows Server 2012 R2 are affected by a vulnerability in the Remote Desktop Services protocol that gives attackers, connected to a remote system via RDP, a way to gain file system access on the machines of other connected users.

Threat actors that exploit the flaw can view and modify clipboard data or impersonate the identities of other users logged in to the machine in order to escalate privileges or to move laterally on the network, researchers from CyberArk discovered recently. They reported the issue to Microsoft, which issued a patch for the flaw (CVE-2022-21893) in its security update for January this Tuesday.

https://www.darkreading.com/vulnerabilities-threats/rdp-bug-enables-data-theft-smartcard-hijacking

*Click above link to read more.*

Back to top

---

### High-severity vulnerability in 3 WordPress plugins affected 84,000 websites

Researchers have disclosed a security shortcoming affecting three different WordPress plugins that impact over 84,000 websites and could be abused by a malicious actor to take over vulnerable sites.

"This flaw made it possible for an attacker to update arbitrary site options on a vulnerable site, provided they could trick a site's administrator into performing an action, such as clicking on a link," WordPress security company Wordfence said in a report published last week.

https://thehackernews.com/2022/01/high-severity-vulnerability-in-3.html

*Click above link to read more.*

Back to top

---

### AWS Glue flaw let attackers access AWS customer accounts

An AWS Glue security flaw has been identified and addressed in Amazon Web Services (AWS) recently by the cybersecurity researchers at Orca security firm.

But, what is AWS Glue? It is a serverless cloud data integration service that generally helps users to do the following things:

- Discover data for app development,
- Prepare data for app development,
- Combine data for app development,
- Machine learning, and
- Analytics.

https://cybersecuritynews.com/aws-glue-flaw/

*Click above link to read more.*

Back to top

---

### DHL dethrones Microsoft as most imitated brand in phishing attacks

DHL was the most imitated brand in phishing campaigns throughout Q4 2021, pushing Microsoft to second place, and Google to fourth.

This isn't surprising considering that the final quarter of every year includes the Black Friday, Cyber Monday, and Christmas shopping season, so phishing lures based on package deliveries naturally increase.

https://www.bleepingcomputer.com/news/security/dhl-dethrones-microsoft-as-most-imitated-brand-in-phishing-attacks/

*Click above link to read more.*

Back to top

---

### How a hacker controlled dozens of Teslas using a flaw in third-party app

A 19-year-old hacker and security researcher said he was able to control some features of dozens of Tesla cars all over the world thanks to a vulnerability in a third-party app that allows car owners to track their car’s movements, remotely unlock doors, open windows, start keyless driving, honk, and flash lights.

David Colombo, the researcher who found the issue, asked Motherboard not to reveal all the details about his findings—such as the name of the third-party app—given that some of the vulnerabilities he discovered are yet to be fixed. Colombo allowed Motherboard to review his upcoming blog post, which contained the details.

https://www.vice.com/en/article/akv7z5/how-a-hacker-controlled-dozens-of-teslas-using-a-flaw-in-third-party-app

*Click above link to read more.*

Back to top

---

### 7 strategies to improve cybersecurity in 2022

The cyber security landscape is always changing. As the cyber threats continue to evolve, so do cyber strategies for combating them. With cyber security being one of the most popular topics in business today, it's essential that you stay on top of the latest trends and best practices to ensure your organization stays secure. In this post, we will discuss 7 cyber security trends coming in 2022 that every business should be aware of!

https://www.newsanyway.com/2022/01/18/7-strategies-to-improve-cybersecurity-in-2022/

*Click above link to read more.*

Back to top

---

### Cyberattacks surge amid accelerating pace of Covid-driven digitalisation: WEF study

The accelerating pace of digitalisation, fuelled by the Covid-19 pandemic, has led to a record-breaking year for cybercrime with ransomware attacks rising 151% in 2021, and an average of 270 cyberattacks per organisation being faced, a new study showed on Tuesday.

The World Economic Forum's 'Global Cybersecurity Outlook 2022', released during its online Davos Agenda summit, further said that each successful cyber breach cost a company $3.6 million (nearly Rs 27 crore) last year, while the average share price of the hacked company underperformed NASDAQ by nearly 3% even six months after the event in case of the breach becoming public.

https://economictimes.indiatimes.com/tech/technology/cyberattacks-surge-amid-accelerating-pace-of-covid-driven-digitalisation-wef-study/articleshow/88971332.cms

*Click above link to read more.*

Back to top

---

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

********************************************************************************

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer