




February 15, 2022

Challenge yourself with our [Love Security](#) quiz!

[This past week's stories:](#)

-  [CIRA report warns Canadians of cryptocurrency and streaming sites](#)
-  [UBC Medicine reports 'serious cyber security attack' after phishing incident](#)
-  [Significant gaps, data at risk in government systems, says security committee](#)
- [Credential-stuffing attacks on remote Windows systems took off in 2021](#)
- [Linux malware on the rise](#)
- [Iranian APT group uses previously undocumented Trojan for destructive access to organizations](#)
- [74% of ransomware revenue goes to Russia-linked hackers](#)
- [Ransomware gang says it has hacked 49ers football team](#)
- [Top five risks facing Canadian businesses in 2022](#)
- [Cyber attack: Gloucester council sets aside £380k for IT repairs](#)
- [Could biology hold the clue to better cybersecurity?](#)
- [Personal data compromised in RDS cyber attack](#)
- [Log4j isn't just a cybersecurity threat—it reveals blind spots in our cyber governance](#)

CIRA report warns Canadians of cryptocurrency and streaming sites

CIRA has released the second edition of its Canadian Shield Insights report to educate Canadians on cyber threats.

The organization says that the last few months of 2021 have seen a flood of cyber incidents affecting critical infrastructure as well as individual users ranging from online investment scams in Alberta to false Canada Border Services Agency requests for social insurance numbers.

<https://www.canadiansecuritymag.com/cira-report-warns-canadians-of-cryptocurrency-and-streaming-sites/>

Click above link to read more.

[Back to top](#)

UBC Medicine reports ‘serious cyber security attack’ after phishing incident

A fraudulent email making false allegations against a student was sent to some members of the faculty of medicine.

Gráinne McElroy, the deputy chief information officer in the faculty of medicine, alerted students, faculty and staff of the “serious cyber security attack” in an email Friday morning.

<https://ubyssey.ca/news/ubc-medicine-reports-serious-cyber-security-attack-after-phishing-incident/>

Click above link to read more.

[Back to top](#)

Significant gaps, data at risk in government systems, says security committee

The committee of MPs and senators which oversees federal security policy has uncovered gaps in Canada’s cyberdefences that could leave many agencies vulnerable to state-sponsored hackers from countries like China and Russia.

In a new report, the National Security and Intelligence Committee of Parliamentarians says cyberthreats to government systems and networks are a significant risk to Canada’s security and government operations.

<https://globalnews.ca/news/8620551/data-risk-government-systems/>

Click above link to read more.

[Back to top](#)

Credential-stuffing attacks on remote Windows systems took off in 2021

Password-guessing became last year’s weapon of choice, as attackers attempted to brute-force vulnerable Remote Desktop Protocol (RDP) servers, SQL databases, and SMB file shares.

Attackers have increasingly targeted remote Windows systems, fueling a surge in credential-stuffing attacks against systems running the remote desktop protocol (RDP), which jumped nearly ninefold in 2021, according to new data.

A report published by ESET this week shows password-based attacks hit European countries the hardest — particularly, Spain, Italy, France, and Germany — accounting for 116 billion of the 288 billion RDP attacks detected by ESET in 2021. While attackers mainly targeted RDP servers, they also sent billions of log-in attempts to database and file-sharing servers, according to the report.

https://www.darkreading.com/endpoint/credential-stuffing-attacks-on-remote-windows-systems-took-off-in-2021?_sp=2785677c-e470-4245-ade3-599289753735.1644627853168

Click above link to read more.

[Back to top](#)

Linux malware on the rise

With Linux frequently used as the basis for cloud services, virtual-machine hosts, and container-based infrastructure, attackers have increasingly targeted Linux environments with sophisticated exploits and malware.

New analysis, based on telemetry collected from attacks on VMware customers, shows an increasing number of ransomware programs targeting Linux hosts to infect virtual-machine images or containers; more use of cryptojacking to monetize illicit access; and more than 14,000 instances of Cobalt Strike — 56% of which are pirated copies used by criminals or thrifty companies that have not bought licenses. The red-team tool has become so popular as a way to manage compromised machines that underground developers created their own protocol-compatible version of the Windows program for Linux, VMware states in a newly released report, "Exposing Malware in Linux-based Multi-Cloud Environments."

<https://www.darkreading.com/cloud/linux-malware-on-the-rise-including-illicit-use-of-cobalt-strike>

Click above link to read more.

[Back to top](#)

Iranian APT group uses previously undocumented Trojan for destructive access to organizations

Researchers have come across a previously undocumented Trojan used by an APT group of Iranian origin that has been targeting organizations in Israel but also other countries since last year with the intention of damaging their infrastructure.

The group, tracked as Moses Staff by researchers from security firm Cybereason, has been operating since at least September 2021 and its primary goal is to steal sensitive data. It also deploys file encrypting malware, but unlike ransomware, the goal is to cause business disruption and cover its tracks rather than financial gain.

<https://www.csoonline.com/article/3649209/iranian-apt-group-uses-previously-undocumented-trojan-for-destructive-access-to-organizations.html>

Click above link to read more.

[Back to top](#)

74% of ransomware revenue goes to Russia-linked hackers

Researchers say more than \$400 million worth of crypto-currency payments went to groups "highly likely to be affiliated with Russia".

Russia has denied accusations that it is harbouring cyber-criminals.

Researchers also claim "a huge amount of crypto-currency-based money laundering" goes through Russian crypto-companies.

<https://www.bbc.com/news/technology-60378009>

Click above link to read more.

[Back to top](#)

Ransomware gang says it has hacked 49ers football team

The San Francisco 49ers have been hit by a ransomware attack, with cyber criminals claiming they stole some of the football team's financial data.

The ransomware gang BlackByte recently posted some of the purportedly stolen team documents on a dark web site in a file marked "2020 Invoices." The gang did not make any of its ransom demands public or specify how much data it had stolen or encrypted.

<https://apnews.com/article/san-francisco-49ers-nfl-sports-technology-europe-370239b9281caea114b3162be54b028e>

Click above link to read more.

[Back to top](#)

Top five risks facing Canadian businesses in 2022

As the COVID-19 pandemic continues to pose significant challenges to the country's supply chains, business interruption remains the top concern for many Canadian companies, a new report from Allianz Global Corporate & Specialty (AGCS) reveals.

For its Risk Barometer 2022 survey, the insurance giant interviewed 2,650 corporate risk experts from 89 countries and territories – including Canada – to find out what these professionals perceived to be the biggest threats facing businesses this year.

<https://www.insurancebusinessmag.com/ca/news/professional-liability/top-five-risks-facing-canadian-businesses-in-2022-325383.aspx>

Click above link to read more.

[Back to top](#)

Cyber attack: Gloucester council sets aside £380k for IT repairs

Council leaders are setting aside £380,000 to help restore IT systems affected by a cyber attack.

Gloucester City Council discovered its systems had been breached in December.

The attack, which has been linked to hackers in Russia, affected online revenue and benefits, planning and customer services.

<https://www.bbc.com/news/uk-england-gloucestershire-60360231>

Click above link to read more.

[Back to top](#)

Could biology hold the clue to better cybersecurity?

Advances in cybersecurity have come fast and furious in recent years. Yet, despite all the gains, there has never been more pain. Hacking, cracking, and attacking techniques are more sophisticated than ever, and more and more organizations are succumbing to breaches and breakdowns.

<https://www.darkreading.com/the-cyber-future/does-biology-hold-the-clue-to-better-cybersecurity->

Click above link to read more.

[Back to top](#)

Personal data compromised in RDS cyber attack

Personal data belonging to staff, members and suppliers of the Royal Dublin Society was compromised during a cyber attack last week.

The RDS said it became aware it was the victim of a ransomware attack on 8 February, during which data was extracted from servers, before it was encrypted to make it inaccessible to the RDS.

In a statement today, the RDS said immediate steps were taken to restore the systems, reinforce existing security and mitigate the potential impact.

<https://www.rte.ie/news/2022/0215/1280931-rds-cyberattack/>

Click above link to read more.

[Back to top](#)

Log4j isn't just a cybersecurity threat—it reveals blind spots in our cyber governance

CISOs already have plenty of IT vulnerabilities to worry about, so when the Log4j vulnerability was announced in December—well, how significant can one more crisis be on top of your already-long list, right?

Wrong. Log4j is more than an urgent cybersecurity threat. It also neatly captures many of the IT security and compliance challenges that businesses face today. So even as CISOs scramble to remove all the Log4j threats in your IT ecosystem, we should also consider why Log4j is such a pressing problem.

<https://securityboulevard.com/2022/02/log4j-isnt-just-a-cybersecurity-threat-it-reveals-blind-spots-in-our-cyber-governance/>

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.

