



May 25, 2021

Challenge yourself with our [Spotting a Fake](#) quiz!

[This week's stories:](#)

 [Ransomware a 'scourge' that needs international action, RSA Conference told](#)

 [HBC takes top spot in cyber skills competition](#)

[Doncaster insurance firm One Call hit by not-dead-at-all Darkside ransomware gang](#)

[Colonial Pipeline take-away for CISOs: Embrace the mandates](#)

[Fraudsters employ Amazon 'vishing' attacks in fake order scams](#)

[AXA ransomware attack comes just days after insurer pulled coverage for cyber-attack class in France](#)

[Apple Exec Calls Level of Mac Malware 'Unacceptable'](#)

[Microsoft warns of malware campaign spreading a RAT masquerading as ransomware](#)

[23 Android Apps Expose Over 100,000,000 Users' Personal Data](#)

[Report finds 10% of pharma manufacturers at high risk for ransomware](#)

Ransomware a 'scourge' that needs international action, RSA Conference told

Ransomware is a "scourge" that has to be fought by governments around the world, according to experts who spoke at the annual RSA Conference this week.

"This is a threat that has moved from economic nuisance eight years ago to national security and public health and safety threat today," Michael Daniel, CEO of the Cyber Threat Alliance and a former White House cybersecurity co-ordinator, told a panel.

<https://www.itworldcanada.com/article/ransomware-a-scourge-that-needs-international-action-rsa-conference-told/447542>

Click above link to read more.

[Back to top](#)

HBC takes top spot in cyber skills competition

Canadian retailer the Hudson's Bay Company recently took first place in the International Cyber League (ICL), organized by Cyberbit, a cyber skilling platform headquartered in Ra'anana, Israel.

<https://www.canadiansecuritymag.com/hbc-takes-top-spot-in-cyber-skills-competition/>

Click above link to read more.

[Back to top](#)

Doncaster insurance firm One Call hit by not-dead-at-all Darkside ransomware gang

A Doncaster insurance company has been hit by ransomware from the Darkside crew – whose "press release" declaring it was shutting down its operations last week was taken at face value by some pundits.

The Doncaster Free Press reports that One Call Insurance, based in the northern English city, had been compromised by Darkside a week ago.

https://www.theregister.com/2021/05/21/darkside_ransomware_doncaster/?&web_view=true

Click above link to read more.

[Back to top](#)

Colonial Pipeline take-away for CISOs: Embrace the mandates

The DarkSide attack on Colonial is yet another wake-up call for companies to harden their systems against ransomware. History suggests that might not happen despite new government guidance.

<https://www.csoonline.com/article/3618762/colonial-pipeline-take-away-for-cisos-embrace-the-mandates.html>

Click above link to read more.

[Back to top](#)

Fraudsters employ Amazon 'vishing' attacks in fake order scams

Case studies highlight how scam artists are using voice messages to dupe their victims into handing over credentials or cash.

Researchers have highlighted tactics used by fraudsters today in voice-based phishing campaigns.

Phishing attempts involve fraudulent messages sent over email, social media networks, SMS, and other text-based platforms. They may appear to be from your bank, popular online services -- such as PayPal or Amazon -- or they may attempt to lure in victims with promises of tax rebates and competition prizes.

<https://www.zdnet.com/article/fraudsters-employ-amazon-vishing-attacks-in-fake-order-scams/>

Click above link to read more.

[Back to top](#)

AXA ransomware attack comes just days after insurer pulled coverage for cyber-attack class in France

Insurance giant AXA has been hit by a massive ransomware attack, just days after announcing that it would no longer cover damage from that class of cyber-attack in France.

The attack – targeted against AXA’s Asia Assistance division – hit IT operations in Thailand, Malaysia, Hong Kong, and the Philippines.

<https://portswigger.net/daily-swig/axa-ransomware-attack-comes-just-days-after-insurer-pulled-coverage-for-cyber-attack-class-in-france>

Click above link to read more.

[Back to top](#)

Apple Exec Calls Level of Mac Malware ‘Unacceptable’

Apple is using the growing threat of malware on its Mac platform as a defense in a lawsuit that could force the company to open up new channels of applications for its mobile iOS platform.

In testimony in a California court Wednesday, Apple head of software engineering, Craig Federighi called the level of malware threat against the Mac platform one that the company finds “unacceptable” and continue to defend against with restrictive application-distribution platforms, according to a published report on CNET.

<https://threatpost.com/apple-mac-malware-unacceptable/166340/>

Click above link to read more.

[Back to top](#)

Microsoft warns of malware campaign spreading a RAT masquerading as ransomware

The Microsoft security team has published details on Wednesday about a malware campaign that is currently spreading a remote access trojan named STRRAT that steals data from infected systems while masquerading as a ransomware attack.

According to the Microsoft Security Intelligence team, the campaign is currently leveraging a mass-spam distribution vector to bombard users with emails containing malicious PDF file attachments.

<https://therecord.media/microsoft-warns-of-malware-campaign-spreading-a-rat-masquerading-as-ransomware/>

Click above link to read more.

[Back to top](#)

23 Android Apps Expose Over 100,000,000 Users' Personal Data

Misconfigurations in multiple Android apps leaked sensitive data of more than 100 million users, potentially making them a lucrative target for malicious actors.

"By not following best-practices when configuring and integrating third-party cloud-services into applications, millions of users' private data was exposed," Check Point researchers said in an analysis published today and shared with The Hacker News.

https://thehackernews.com/2021/05/these-23-android-apps-expose-over.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29/

Click above link to read more.

[Back to top](#)

Report finds 10% of pharma manufacturers at high risk for ransomware

The cyber risk platform Black Kite released a new report this week finding that one in 10 global pharmaceutical manufacturers are at a high risk of suffering a ransomware attack.

The report, published on Tuesday, evaluated the cybersecurity posture of the 200 largest global pharmaceutical companies and 166 associated third-party vendors.

<https://www.healthcareitnews.com/news/report-finds-10-pharma-manufacturers-high-risk-ransomware>

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



OCIO

Office of the
Chief Information Officer