


June 28, 2022

Challenge yourself with our Phishing quiz!

This past week's stories:

 **Cybersecurity framework still not finalized after 3 years, N.L. agency blames COVID for delay**

 **UWindsor experiencing computer systems outage, 'cybersecurity incident' to blame**

Top 10 cybersecurity lingo to keep a tab on in 2022

Yodel parcel company confirms cyberattack is disrupting delivery

Ransomware-as-a-Service: Learn to enhance cybersecurity approaches

Russian hackers exploiting Microsoft Follina vulnerability against Ukraine

IOTW: CISA reveals 130GB Log4shell breach

Hackers stole \$100 million in the latest crypto theft

Attackers keep targeting VMware Horizon, exploiting unpatched Log4Shell

Apple and Android phones hacked by Italian spyware, says Google

Study: Co.'s 'not confident' in ability to handle cyber-attack

How much does it cost to orchestrate a cyberattack in 2022?

Cybersecurity experts warn of emerging threat of "Black Basta" ransomware

Breaking down the Zola hack and why password reuse is so dangerous

Cybersecurity framework still not finalized after 3 years, N.L. agency blames COVID for delay

The Newfoundland and Labrador Centre for Health Information is defending the fact that its cybersecurity framework has remained in draft format for nearly three years and is still not finalized.

The framework was drafted in 2019, when all technical support for the province's four regional health authorities was transitioning into a "shared-service model" under NLCHI.

<https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cybersecurity-framework-draft-nlchi-1.6494354>

Click above link to read more.

[Back to top](#)

UWindsor experiencing computer systems outage, 'cybersecurity incident' to blame

The University of Windsor is dealing with a system outage which has shut down many of the school's online platforms for the past three days.

Staff is working to restore an "unexpected but significant and prolonged" systems outage that started on Monday, according to the University.

<https://windsor.ctvnews.ca/uwindsor-experiencing-computer-systems-outage-cybersecurity-incident-to-blame-1.5958072>

Click above link to read more.

[Back to top](#)

Top 10 cybersecurity lingo to keep a tab on in 2022

Cybersecurity is the practice of protecting systems, networks, and programs from cyberattacks. The practice is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses. With an increasing number of users, devices, and programs in the modern enterprise, combined with the increasing deluge of data much of which is sensitive or confidential the importance of cybersecurity continues to grow. Within the context of cybersecurity, certain lingo are starting to make their way into mainstream conversation and news, hinting at the increased importance of cybersecurity in our daily work and life. So, here we lay out our top 10 cybersecurity lingo that might come in handy in your next conversation.

<https://www.analyticsinsight.net/top-10-cybersecurity-lingo-to-keep-a-tab-on-in-2022/>

Click above link to read more.

[Back to top](#)

Yodel parcel company confirms cyberattack is disrupting delivery

Services for the U.K.-based Yodel delivery service company have been disrupted due to a cyberattack that caused delays in parcel distribution and tracking orders online.

The company has not published any details about the incident, such as when it occurred or its nature but implies that customer payment information has not been affected since it is neither stored on its systems nor processed by them.

<https://www.bleepingcomputer.com/news/security/yodel-parcel-company-confirms-cyberattack-is-disrupting-delivery/>

Click above link to read more.

[Back to top](#)

Ransomware-as-a-Service: Learn to enhance cybersecurity approaches

Ransomware-as-a-Service is a new form of malicious and subscription-based business model involving the selling or renting of ransomware to buyers. The operator is known for providing the ransomware payload as well as infrastructure to boost the time to value for the ransomware-as-a-Service affiliate.

Ransomware-as-a-Service follows a similar cyberattack pattern in weak links of computer systems. The affiliate tries to gain access to onboarding documentation to track the progress of cyberattacks. Cybercriminals use Initial Access Broker (IAB) services for network access. It makes it easier for them to perform data theft, ransomware payload deployment, and many more.

<https://www.analyticsinsight.net/ransomware-as-a-service-learn-to-enhance-cybersecurity-approaches/>

Click above link to read more.

[Back to top](#)

Russian hackers exploiting Microsoft Follina vulnerability against Ukraine

The Computer Emergency Response Team of Ukraine (CERT-UA) has [cautioned](#) of a new set of spear-phishing attacks exploiting the "Follina" flaw in the Windows operating system to deploy password-stealing malware.

Attributing the intrusions to a Russian nation-state group tracked as APT28 (aka Fancy Bear or Sofacy), the agency said the attacks commence with a lure document titled "Nuclear Terrorism A Very Real Threat.rtf" that, when opened, exploits the recently disclosed vulnerability to download and execute a malware called CredoMap.

<https://thehackernews.com/2022/06/russian-hackers-exploiting-microsoft.html>

Click above link to read more.

[Back to top](#)

IOTW: CISA reveals 130GB Log4shell breach

First discovered in December 2021, the Log4Shell vulnerability continues to be exploited by threat actors as highlighted by a joint advisory by the Cybersecurity and Infrastructure Security Agency (CISA) and United States Coast Guard Cyber Command (CGCYBER) on 23 June.

Cyber threat actors have exploited unpatched, public-facing VMware Horizon, a virtual desktop provider, and Unified Access Gateway (UAG) servers to gain initial access to networks, the joint advisory said.

<https://www.cshub.com/attacks/news/iotw-cisa-reveals-130gb-log4shell-breach>

Click above link to read more.

[Back to top](#)

Hackers stole \$100 million in the latest crypto theft

Harmony, a California-based crypto firm, announced on Thursday night that hackers have stolen \$100 million worth of cryptocurrency from one of its blockchain bridges.

The company said on Twitter that it has partnered up with law enforcement and forensic specialists to try to identify the hackers and retrieve the stolen funds.

<https://thehill.com/policy/cybersecurity/3536352-hackers-stole-100-million-in-latest-crypto-theft/>

Click above link to read more.

[Back to top](#)

Attackers keep targeting VMware Horizon, exploiting unpatched Log4Shell

Malicious actors continue to dog VMware Horizon and Unified Access Gateway server deployments, capitalizing on unpatched Log4Shell, the Cybersecurity and Infrastructure Security Agency said Thursday in a joint advisory with the U.S. Coast Guard Cyber Command.

The agencies are calling for organizations to update all VMware Horizon and UAG systems and, if fixes weren't applied in Dec. 2021, organizations should consider their systems compromised and start threat hunting.

<https://www.cybersecuritydive.com/news/vmware-horizon-log4shell-cisa/626038/>

Click above link to read more.

[Back to top](#)

Apple and Android phones hacked by Italian spyware, says Google

An Italian company's hacking tools were used to spy on Apple and Android smartphones in Italy and Kazakhstan, Alphabet Inc's Google said in a new report.

Milan-based RCS Lab, whose website claims European law enforcement agencies as clients, developed tools to spy on private messages and contacts of the targeted devices, the report said.

European and American regulators have been weighing potential new rules over the sale and import of spyware.

<https://www.theguardian.com/technology/2022/jun/23/apple-and-android-phones-hacked-by-italian-spyware-says-google>

Click above link to read more.

[Back to top](#)

Study: Co.'s 'not confident' in ability to handle cyber-attack

After nearly three years of a business model shift, inevitable digital transformation, and countless ransomware attacks, most leaders are no longer confident in their ability to manage cyber risk compared to two years ago.

That's according to a new report released by insurance broker and risk consultant Marsh and Microsoft Corp.

"The State of Cyber Resilience" report surveyed more than 660 cyber risk decision makers globally and 162 in Latin America to analyze how cyber risk is viewed by various executives from leading organizations, including cyber security, IT, risk and insurance management, finance, and executive leadership.

<https://newsismybusiness.com/study-co-s-not-confident-in-ability-to-handle-cyber-attack/>

Click above link to read more.

[Back to top](#)

How much does it cost to orchestrate a cyberattack in 2022?

How much does it cost to orchestrate a cyber attack in 2022? Truthfully, not a lot. For less than \$100, you can probably subscribe to a lifetime's supply of cyber attacks on the targets of your choosing. Really.

Better still, the sign-up process couldn't be simpler these days. All you'll need is an email address and a payment card (or cryptocurrency). No dark web, balaclavas and voice-changers, nor direct human interaction with criminals required.

<https://www.ft.com/content/2b8dbbb3-ff4b-49bf-8b2a-1d149103abcf>

Click above link to read more.

[Back to top](#)

Cybersecurity experts warn of emerging threat of "Black Basta" ransomware

The Black Basta ransomware-as-a-service (RaaS) syndicate has amassed nearly 50 victims in the U.S., Canada, the U.K., Australia, and New Zealand within two months of its emergence in the wild, making it a prominent threat in a short window.

"Black Basta has been observed targeting a range of industries, including manufacturing, construction, transportation, telcos, pharmaceuticals, cosmetics, plumbing and heating, automobile dealers, undergarments manufacturers, and more," Cybereason said in a report.

<https://thehackernews.com/2022/06/cybersecurity-experts-warn-of-emerging.html>

Click above link to read more.

[Back to top](#)

Breaking down the Zola hack and why password reuse is so dangerous

In May of 2022, the wedding planning and registry site Zola suffered a major security breach. Hackers managed to gain access to user accounts and attempted to place gift card orders using funds tied to the compromised accounts.

Thankfully, Zola refunded all of the fraudulent gift card orders and none of Zola's customers lost money as a result of the attack. Even so, it is worth examining how the attack happened and what could have been done to prevent the attack.

<https://www.bleepingcomputer.com/news/security/breaking-down-the-zola-hack-and-why-password-reuse-is-so-dangerous/>

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.

