November 16, 2021

Challenge yourself with our Online Shopping quiz!

This week's stories:

Some patient, employee information, accessed in N.L. cyberattack, government says

The Newfoundland and Labrador government revealed Tuesday that whoever was behind a cyberattack that has hobbled its health-care system managed to obtain personal information of patients and employees.

Government officials told a briefing that some patient and employee information from two health authorities was accessed through an online data repository. They don't know how many people were affected.

https://www.canadiansecuritymag.com/some-patient-employee-information-accessed-in-n-l-cyberattack-government-says/

Click above link to read more.

Back to top

Ottawa clinic paralyzed by cyber security “incident”

The IT systems of the Rideau Valley Health Centre in Ottawa, ON have been effectively disabled due to a cybersecurity incident – the specifics of which have yet to be disclosed.

The cyber incident put a hold on the clinic’s capability to schedule appointments, and also affected Rideau Valley Health Centre’s phone services. The clinic announced that it is working to fix the issue immediately.

https://www.insurancebusinessmag.com/ca/news/cyber/ottawa-clinic-paralyzed-by-cybersecurity-incident-316505.aspx

Click above link to read more.

Back to top

Hack leaves fertility clinic medical data at risk

Data from a private fertility clinic was put at risk after a ransomware attack hit a document management firm.

The Lister Fertility Clinic said the firm, which it used for scanning medical records, had been "hacked" by a"cyber-gang", in a letter sent to about 1,700 patients.

Stor-a-file Limited said in total 13 organisations had been affected, of which six are healthcare-related.

https://www.bbc.com/news/technology-59156683

Click above link to read more.

Back to top

Critical Citrix DDoS bug shuts down network, cloud app access

The distributed computing vendor patched the flaw, affecting Citrix ADC and Gateway, along with another flaw impacting availability for SD-WAN appliances.

A critical security bug in the Citrix Application Delivery Controller (ADC) and Citrix Gateway could allow cyberattackers to crash entire corporate networks without needing to authenticate.

https://threatpost.com/critical-citrix-bug-etwork-cloud-app-access/176183/

Click above link to read more.

Back to top

New Android Spyware poses Pegasus-like threat

PhoneSpy already has stolen data and tracked the activity of targets in South Korea, disguising itself as legitimate lifestyle apps.

Researchers discovered new Android spyware that provides similar capabilities to NSO Group's Pegasus controversial software. Called PhoneSpy, the mobile surveillance-ware has been spotted activity targeting South Koreans without their knowledge.

https://threatpost.com/new-android-spyware-poses-pegasus-like-threat/176155/

Click above link to read more.

Back to top

Queensland water supplier Sunwater targeted by hackers in months-long undetected cyber security breach

Queensland's largest regional water supplier, Sunwater, says it was targeted by hackers in a cyber security breach that went undetected for nine months.

It has been revealed that hackers left suspicious files on a webserver to redirect visitor traffic to an online video platform last year.

https://www.abc.net.au/news/2021-11-11/qld-hackers-target-water-supplier-sunwater-cyber-security-attack/100610400

Click above link to read more.

Back to top

'We lost festive savings in a family WhatsApp scam'

A grandfather has told of how he lost money saved for Christmas presents after his family were duped by fraudsters on WhatsApp.

The 75-year-old, who wished to remain anonymous, said they had been tricked by criminals posing as his grand-daughter on the messaging service.

He transferred £1,550 to the con-artists, for an emergency medical bill that was a fake.

https://www.bbc.com/news/business-59238425

Click above link to read more.

Back to top

CISA issues advisory about Siemens software vulnerabilities

The U.S. Cybersecurity and Infrastructure Security Agency issued an advisory this week about critical vulnerabilities to software used in medical devices.

As outlined by a blog post from Forescout Research Labs, the set of 13 new vulnerabilities affects Siemens' Nucleus TCP/IP stack.

The flaws potentially allow for remote code execution, denial of service and information leak.
Click above link to read more.

https://www.healthcareitnews.com/news/cisa-issues-advisory-about-siemens-software-vulnerabilities

Back to top

Millions of routers, IoT devices at risk from new open-source malware

BotenaGo, written in Google's Golang programming language, can exploit more than 30 different vulnerabilities.

Newly surfaced malware that is difficult to detect and written in Google's open-source programming language has the potential to exploit millions of routers and IoT devices, researchers have found.

Discovered by researchers at AT&T AlienLabs, BotenaGo can exploit more than 30 different vulnerabilities to attack a target, Ofer Caspi, a security researcher at Alien Labs, wrote in a blog post published Thursday.

https://threatpost.com/routers-iot-open-source-malware/176270/

Click above link to read more.

Back to top

Palo Alto Warns of zero-day bug in firewalls let hackers execute an arbitrary code remotely

A Zero-Day vulnerability has been identified by the Massachusetts-based cybersecurity firm Randori in Palo Alto Networks firewalls using GlobalProtect VPN.

This Zero-Day flaw could be exploited by an unauthorized attacker to execute arbitrary code remotely on vulnerable devices with superuser privileges. This Zero-Day bug was tracked as CVE-2021-3064 scored 9.8 on the CVSS and affects the PAN-OS 8.1 and earlier than PAN-OS 8.1.17.

https://cybersecuritynews.com/palo-alto-warns-of-zero-day-bug/

Click above link to read more.

Back to top

Open source project aims to detect living-off-the-land attacks

Attackers who use standard system commands during a compromise — a technique known as living off the land (LotL) — to avoid detection by defenders and endpoint security software may find their activities in the spotlight if a machine learning project open sourced by software firm Adobe this week bears fruit.

The project, dubbed LotL Classifier, uses supervised learning and an open source dataset of real-world attack to extract features of specific commands and then classifies the command based on a features extracted using human analysis as a model. Those features are then used to determine whether the command is good or bad and to label the command with a set of tags that can be used for anomaly detection.

https://www.darkreading.com/threat-intelligence/open-source-project-aims-to-detect-living-off-the-land-attacks

Click above link to read more.

Back to top

Researchers demonstrate new fingerprinting attack on tor encrypted traffic

A new analysis of website fingerprinting (WF) attacks aimed at the Tor web browser has revealed that it's possible for an adversary to glean a website frequented by a victim, but only in scenarios where the threat actor is interested in a specific subset of the websites visited by users.

"While attacks can exceed 95% accuracy when monitoring a small set of five popular websites, indiscriminate (non-targeted) attacks against sets of 25 and 100 websites fail to exceed an accuracy of 80% and 60%, respectively," researchers Giovanni Cherubin, Rob Jansen, and Carmela Troncoso said in a newly published paper.

https://thehackernews.com/2021/11/researchers-demonstrate-new.html

Click above link to read more.

Back to top

Fake emails exploited FBI email service to warn of phony cyberattacks

The FBI is usually a key source that tries to help people combat cyberattacks and security threats. But in an unusual twist, the law enforcement agency has found itself the victim of an exploit.

On Saturday, spam tracker Spamhaus tweeted that it had learned of "scary" emails being sent purportedly from the FBI and Department of Homeland Security (DHS). One such email warned the recipient that they were hit by a sophisticated chain attack, potentially causing severe damage to their infrastructure. Though the emails were sent from a portal owned by the FBI and DHS, Spamhaus said that the messages themselves were fake.

https://www.techrepublic.com/article/fake-emails-exploited-fbi-email-service-to-warn-of-phony-cyberattacks/

Click above link to read more.

Back to top

****

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