November 2, 2021

Security Day is Tomorrow! Remember to sign up!

Challenge yourself with our Online Shopping quiz!

This week's stories:

- Some Toronto transit online services down after ransomware attack
- Suspected cyberattack in N.L. hits 'brain' of province's health care system
- IBM Canada, U of Ottawa to establish Cyber Range to train for cybersecurity threats
- Hackers breach iOS 15, Windows 10, Google Chrome during massive cyber security onslaught
- Multinational police force arrests 12 suspected hackers
- Free tool scans web servers for vulnerability to HTTP header-smuggling attacks
- New 'Trojan Source' technique lets hackers hide vulnerabilities in source code
- Hackers upping SSL usage for encrypted attacks, communications
- Suspected REvil gang insider identified
- Russian cyberspies target cloud services providers and resellers to abuse delegated access
- How disinformation creates insider threats
- Hackers attacking Windows using infostealer malware by Mimics as Legitimate Win 10 App
- Deloitte: 14% of U.S. orgs remain defenseless as cybersecurity threats loom
- Man charged with hacking MLB, NBA, NFL, and NHL user accounts to stream games

---

Some Toronto transit online services down after ransomware attack

Toronto's public transit authority is reporting outages in some of its online services following a ransomware attack that targeted the agency earlier in the week.

The Toronto Transit Commission, which operates the city's bus, subway, streetcar and paratransit services, has been dealing with the attack on its computer systems since Thursday.

https://www.canadiansecuritymag.com/some-toronto-transit-online-services-down-after-ransomware-attack/

Click above link to read more.

Back to top

Suspected cyberattack in N.L. hits 'brain' of province's health care system

ST. JOHN'S, N.L. — A suspected cyberattack on Newfoundland and Labrador's health network has led to the cancellation of thousands of medical appointments across the province and forced some local health systems to revert to paper.

The "brain" of the network's data centre, operated by Bell, has been damaged, including the main and backup computer systems, Health Minister John Haggie told reporters Monday. He said the "possible cyberattack by a third party" was first detected Saturday.

https://www.canadiansecuritymag.com/suspected-cyberattack-in-n-l-hits-brain-of-provinces-health-care-system/

Click above link to read more.

Back to top

IBM Canada, U of Ottawa to establish Cyber Range to train for cybersecurity threats

IBM and the University of Ottawa announced a multi-year partnership to build and operate a Cyber Range: a fully immersive, interactive, and experiential learning facility that will enable research and training in cybersecurity and cyber safety. As part of the agreement, IBM is also making a more than $21 million in-kind contribution to the University over five years to support business development and security training, while uOttawa will invest nearly $7 million over the same period.

https://www.canadiansecuritymag.com/ibm-canada-u-of-ottawa-to-establish-cyber-range-to-train-for-cybersecurity-threats/

Click above link to read more.

Back to top

Hackers breach iOS 15, Windows 10, Google Chrome during massive cyber security onslaught

During the weekend of 16-17 October, Chinese hackers went on something of a rampage that saw all but three of the 15 target products breached during the exploit onslaught that was the Tianfu Cup. This annual competition, held in the Sichuan province of Chengdu, has been the go-to for China's elite hackers since they were banned from participating in similar competitive hacking events outside of the country. The biggest and best known of these, Pwn2Own, is due to take place in Austin, Texas, 2-5 November, and I will be reporting on that next weekend when the results are known.

In the meantime, what of the massive Tianfu Cup cybersecurity onslaught? Well, I've already reported how the iPhone 13 Pro, running a fully patched (at the time) version of iOS 15.0.2, was breached not once but twice. The zero-day vulnerabilities, exploited by the Kunlun Lab and Team Pangu in a matter of seconds on the day, saw a remote code execution attack and the first iOS 15 jailbreak.

https://www.forbes.com/sites/daveywinder/2021/10/30/hackers-breach-ios-15-windows-10-google-chrome-during-massive-cyber-security-onslaught/?sh=74e6a6d62f62

Click above link to read more.

Back to top

Multinational police force arrests 12 suspected hackers

Europol on Friday announced the arrest of 12 individuals for their suspected roles in ransomware attacks against critical infrastructure across the world.

These actors are believed to have affected more than 1,800 victims in 71 countries and are known to have targeted large corporations causing business disruption.

https://www.bankinfosecurity.com/multinational-police-force-arrests-12-suspected-hackers-a-17828

Click above link to read more.

Back to top

Free tool scans web servers for vulnerability to HTTP header-smuggling attacks

A researcher has created a method for testing and identifying how HTTP/HTTPS headers can be abused to sneak malicious code into back-end servers.

Daniel Thatcher, researcher and penetration tester at Intruder, will present his new research on so-called HTTP header-smuggling at Black Hat Europe, in London next week. He also will release a free tool for testing Web servers for weaknesses that could allow an attacker to pull off this Web attack.

https://www.darkreading.com/application-security/free-tool-scans-web-servers-for-vulnerability-to-http-header-smuggling-attacks

Click above link to read more.

Back to top

New 'Trojan Source' technique lets hackers hide vulnerabilities in source code

A novel class of vulnerabilities could be leveraged by threat actors to inject visually deceptive malware in a way that's semantically permissible but alters the logic defined by the source code, effectively opening the door to more first-party and supply chain risks.

Dubbed "Trojan Source attacks," the technique "exploits subtleties in text-encoding standards such as Unicode to produce source code whose tokens are logically encoded in a different order from the one in

which they are displayed, leading to vulnerabilities that cannot be perceived directly by human code reviewers," Cambridge University researchers Nicholas Boucher and Ross Anderson said in a newly published paper.

https://thehackernews.com/2021/11/new-trojan-source-technique-lets.html

Click above link to read more.

Back to top

Hackers upping SSL usage for encrypted attacks, communications

Hackers are increasingly turning to secure connections to carry out network breaches and encrypted attacks.

A new report from cloud security vendor Zscaler found that instances of hackers using HTTPS connections were up more than 300% on the year.

https://searchsecurity.techtarget.com/news/252508801/Hackers-upping-SSL-usage-for-encrypted-attacks-communications

Click above link to read more.

Back to top

Suspected REvil gang insider identified

German investigators have identified a deep-pocketed, big-spending Russian billionaire whom they suspect of being a core member of the REvil ransomware gang.

He lolls around on yachts, wears a luxury watch with a Bitcoin address engraved on its dial, and is suspected of buying it all with money he made as a core member of the REvil ransomware gang.

https://threatpost.com/revil-ransomware-core-member/175863/

Click above link to read more.

Back to top

Russian cyberspies target cloud services providers and resellers to abuse delegated access

The group of hackers responsible for the SolarWinds software supply chain attack have continued to seek out ways of indirectly gaining access to enterprise networks by targeting IT and cloud services providers that have admin rights on their customers' systems through virtue of their business relationship.

In a new report this week, Microsoft warns that since May, the group known as Nobelium has targeted over 140 cloud service resellers and technology providers and has succeeded to compromise as many as 14. Nobelium, also known as APT29 or Cozy Bear, is considered the hacking arm of Russia's foreign intelligence service, the SVR.

https://www.csoonline.com/article/3638452/russian-cyberspies-target-cloud-services-providers-and-resellers-to-abuse-delegated-access.html

Click above link to read more.

Back to top

How disinformation creates insider threats

As we enter quarter four of 2021, the idea of disinformation as a cyber threat probably hasn't percolated to the forefront of concerns of many CISOs. Indeed, a Venn diagram would show no overlap of "disinformation" with the words "CISO" or "cyber threat," especially in the United States. Yet there is a significant overlap here, and CISOs will be well served to get ahead of the curve.

https://www.csoonline.com/article/3636993/how-disinformation-creates-insider-threats.html

Click above link to read more.

Back to top

Hackers Attacking Windows Using infostealer malware by mimics as legitimate Win 10 App

A new malicious campaign has been detected recently by Rapid7's Managed Detection and Response (MDR) team and Threat Intelligence and Detection Engineering (TIDE) team in which the hackers are targeting Windows using infostealer malware and delivering fake legitimate-looking Win 10 app.

In this malicious campaign, the threat actors infect the users' systems by using a sophisticated technique that bypasses Windows cybersecurity protections called User Account Control (UAC) by exploiting a Windows environment variable and a native scheduled task.

https://cybersecuritynews.com/hackers-attacking-windows-using-infostealer-malware/

Click above link to read more.

Back to top

Deloitte: 14% of U.S. orgs remain defenseless as cybersecurity threats loom

Even as cybersecurity threats rise, a few American organizations still continue to operate without a defense plan or strategy, Deloitte reported Tuesday.

In its 2021 Future of Cyber survey, the accounting and consulting firm revealed that 98% of U.S. executives said their organizations had experienced at least one cybersecurity incident over the past year — compared to 84% in non-U.S. regions. However, despite the higher rate of incidents, nearly 14% of these executives reported that their firms do not have a cyber threat defense plan. Outside the U.S., just 6% of executives had this response.

https://venturebeat.com/2021/10/26/deloitte-14-of-us-orgs-remain-defenseless-as-cybersecurity-threats-loom/

Click above link to read more.

Back to top

Man charged with hacking MLB, NBA, NFL, and NHL user accounts to stream games

The US Department of Justice has filed charges today against a Minnesota man who hacked MLB, NBA, NFL, and NHL user accounts in order to supply content to a pirate streaming website that he operated.

Charges were levied against Joshua Streit, 30, of St. Louis Park, Minnesota. The DOJ claims that Streit, who went online as "Josh Brody" or "inflx," operated the HeHeStreams website between 2017 and August 2021.

https://therecord.media/man-charged-with-hacking-mlb-nba-nfl-and-nhl-user-accounts-to-stream-games/

Click above link to read more.

Back to top