August 10, 2021

Challenge yourself with our Safe Surfing quiz!

This week's stories:

Remote code execution the most common cyber threat faced by Canadian firms: Report

Canadian cybersecurity teams face a wide range of threats, but the most common vulnerability exploit type is remote code execution (RCE), according to a report from Check Point Software Technologies.

In its annual mid-year attack trends report, which uses data from customers, the company said that in 61 per cent of attacks against Canadian organizations in the first six months of the year, a threat actor either tried to or successfully ran code with system-level privileges on a server.

https://www.itworldcanada.com/article/remote-code-execution-the-most-common-cyber-threat-faced-by-canadian-firms-report/456569

Click above link to read more.

Back to top

Back-to-school shopping scams: Watch out for ads on social media and prices too good to be true

As families get ready for the new school year, the B.C. Better Business Bureau (BBB) is warning of a likely rise in online shopping scams.

Since the start of 2021, the agency has received nearly 400 complaints from people who were duped while shopping online, and with many students soon embarking on new purchases for gadgets and learning devices, the BBB is raising the alarm.

https://bc.ctvnews.ca/mobile/back-to-school-shopping-scams-watch-out-for-ads-on-social-media-and-prices-too-good-to-be-true-1.5539097

Click above link to read more.

Back to top

Ransomware demands and payments reach new highs

Ransomware has evolved into one of the most destructive and damaging forms of cyberattack, resulting in huge financial losses for victimized organizations. And as cybercriminals have gotten bolder and greedier, their ransom demands have skyrocketed. A report released Monday by Palo Alto Networks' threat intelligence team, Unit 42, looks at how and why ransomware prices have soared over the past year.

There's typically a difference between ransom demands and actual payments. A cybercriminal or gang may start off by demanding an exorbitant amount of money from a victim but eventually settle for less following negotiations and other factors.

https://www.techrepublic.com/article/ransomware-demands-and-payments-reach-new-highs/?ftag=TREe01923b&bhid=19662319145962710268575546540229&mid=13467941&cid=712327807

Click above link to read more.

Back to top

Attackers scan for Microsoft Exchange ProxyShell remote code execution vulnerabilities

The Exchange server of Microsoft is one of the popular mail servers, and it runs exclusively on Windows Server operating systems. However, cybercriminals are targeting the Microsoft Exchange, as it is one of the widespread mail servers.

According to the experts of Orange Tsai, the hackers are continuously scanning for the Microsoft Exchange ProxyShell remote code execution vulnerabilities, and it has been initiated after the technical details of the servers were released at the Black Hat conference.

https://cybersecuritynews.com/attackers-scan-for-microsoft-exchange-proxyshell/

Click above link to read more.

Back to top

---

14 vulnerabilities found in widely used TCP/IP stack

Security analysts at Forescout Research and JFrog Security Research have discovered 14 vulnerabilities in NicheStack, a proprietary TCP/IP stack used in a wide range of operational technology (OT) devices from more than 200 manufacturers, including most major industrial automation vendors.

The vulnerabilities — which the researchers have collectively named Infra:Halt — enable remote code execution attacks, denial-of-service attacks, information leaks, DNS cache poisoning, and TCP spoofing. While many of the affected devices are likely to have one or more of the vulnerabilities present in their NicheStack implementation, few are likely to have all of them at the same time.

https://www.darkreading.com/vulnerabilities-threats/14-vulnerabilities-found-in-widely-used-tcp-ip-stack

Click above link to read more.

Back to top

FTC: Phishing campaign targets unemployment benefits & PII

The Federal Trade Commission (FTC) this week warned of a phishing campaign targeting victims' unemployment insurance benefits and personally identifiable information (PII).

Malicious text messages claim that victims must "make necessary corrections" to their unemployment insurance claim, verify their personal information, or reactivate their UI benefits account. The texts include a link that redirects to a fake state workforce agency website, where victims are asked to enter site credentials and personal data such as a Social Security number.

https://www.darkreading.com/attacks-breaches/ftc-phishing-campaign-targets-unemployment-benefits-pii

Click above link to read more.

Back to top

Malicious Android apps try to hijack your Facebook account

Savvy cybercriminals often use social engineering to try to trick people into installing malware or revealing sensitive information. A malicious campaign uncovered by mobile security provider Zimperium found malicious Android apps that employed social engineering tactics to gain access to the Facebook accounts of their victims.

Initially available through both Google Play and third-party stores, the malicious apps have surfaced in at least 140 countries since March 2021, hitting more than 10,000 victims, Zimperium said in a Monday blog post. After Zimperium informed Google of the apps in question, the company removed them from Google Play. However, they're still accessible on third-party stores, which means they're a threat for users who sideload apps from unofficial sources.

https://www.techrepublic.com/article/malicious-android-apps-try-to-hijack-your-facebook-account/?ftag=TRE001a825&bhid=196623191459627102685755465402 29&mid=13468930&cid=712327807

Click above link to read more.

Back to top

New Chinese spyware being used in widespread cyber espionage attacks

A threat actor presumed to be of Chinese origin has been linked to a series of 10 attacks targeting Mongolia, Russia, Belarus, Canada, and the U.S. from January to July 2021 that involve the deployment of a remote access trojan (RAT) on infected systems, according to new research.

The intrusions have been attributed to an advanced persistent threat named APT31 (FireEye), which is tracked by the cybersecurity community under the monikers Zirconium (Microsoft), Judgement Panda (CrowdStrike), and Bronze Vinewood (Secureworks).

https://thehackernews.com/2021/08/new-chinese-spyware-being-used-in.html

Click above link to read more.

Back to top

Critical flaw with Kindle let attacker take full control of the device

CheckPoint Research (CPR) team has found a critical flaw in Amazon's Kindle E-Book Reader that could be potentially exploited to take full control over a user's device, resulting in the theft of sensitive information.

According to Yaniv Balmas, head of cyber research at Check Point mentions, "By sending Kindle users a single malicious e-book, a threat actor could have stolen any information stored on the device, from Amazon account credentials to billing information. The security vulnerabilities allow an attacker to target a very specific audience."

https://cybersecuritynews.com/kindle-flaw/

Click above link to read more.

Back to top

Critical Cisco bug in VPN routers allows remote takeover

A critical security vulnerability in a subset of Cisco Systems' small-business VPN routers could allow a remote, unauthenticated attacker to take over a device – and researchers said there are at least 8,800 vulnerable systems open to compromise.

The critical bug affects the vendor's Dual WAN Gigabit VPN routers. According to the advisory, CVE-2021-1609 exists in the web management interface for the devices, and carries a CVSSv3 vulnerability-severity score of 9.8. It arises due to improper validation of HTTP requests.

https://threatpost.com/critical-cisco-bug-vpn-routers/168449/

Click above link to read more.

Back to top

Synology warns of malware infecting NAS devices with ransomware

Taiwan-based NAS maker Synology has warned customers that the StealthWorker botnet is targeting their network-attached storage devices in ongoing brute-force attacks that lead to ransomware infections.

According to Synology's PSIRT (Product Security Incident Response Team), Synology NAS devices compromised in these attacks are later used in further attempts to breach more Linux systems.

https://www.bleepingcomputer.com/news/security/synology-warns-of-malware-infecting-nas-devices-with-ransomware/

Click above link to read more.

Back to top

Australian govt warns of escalating LockBit ransomware attacks

The Australian Cyber Security Centre (ACSC) warns of an increase of LockBit 2.0 ransomware attacks against Australian organizations starting July 2021.

"ACSC has observed an increase in reporting of LockBit 2.0 ransomware incidents in Australia," Australia's cybersecurity agency said in a security alert issued on Thursday.

According to the agency, LockBit victims also report threats of having data stolen during the attacks leaked online, a known and popular tactic among ransomware gangs to coerce their targets into paying the ransoms.

https://www.bleepingcomputer.com/news/security/australian-govt-warns-of-escalating-lockbit-ransomware-attacks/

Click above link to read more.

Back to top

---

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca