October 26, 2021

Security Day is next Wednesday! Remember to sign up!

Join Cyber Security Awareness Month! It's not too late!

Challenge yourself with our Cyber Security Awareness Month quiz!

This week's stories:

- October is Cyber Security Awareness Month
- Small businesses not too concerned with cyber crime despite increased attempts
- Governments hacked REvil ransomware group & forced to go offline
- 83% of ransomware victims paid the ransom to get their data restored – A shocking report
- Solarwinds hackers are targeting the global IT supply chain, Microsoft says
- Millions of Android users scammed in SMS fraud driven by Tik-Tok Ads
- 7 Ways to lock down enterprise printers
- Google unmasks two-year-old phishing & malware campaign targeting YouTube users
- TeamTNT deploys malicious docker image on Docker Hub
- Nigerian romance scam targeted 100 women – FBI
- Bug in popular WinRAR software could let attackers hack your computer
- How do cyberattackers gain access to health systems? Often via smaller hospitals
- TSA to issue cybersecurity requirements for US rail, aviation sectors
- Attackers hijack Craigslist emails to bypass security, deliver malware

---

October is Cyber Security Awareness Month

Global News Morning's Kahla Evans chats with Dr. Jessica Barker, a Cyber Sociologist, who offers some advice and tips on how to stay safe online.

https://globalnews.ca/video/8285990/october-is-cyber-security-awareness-month

Click above link to read more.

Back to top

Small businesses not too concerned with cyber crime despite increased attempts

Global News Morning's Kahla Evans chats with Dr. Jessica Barker, a Cyber Sociologist, who offers some advice and tips on how to stay safe online.

https://www.canadiansecuritymag.com/small-businesses-not-too-concerned-with-cyber-crime-despite-increased-attempts/

Click above link to read more.

Back to top

Governments hacked REvil ransomware group & forced to go offline

On an active international operation that was executed recently by the US along with the multi-country law enforcement agencies, the Notorious ransomware group REvil themselves became the target of hacking and were forced to curtail their activities on the network.

The direct victims of the Russian-led criminal gang include top meatpacker JBS (JBSS3.SA), and the Colonial Pipeline. But, right now after this chasing incident the website of the REvil ransomware group known as "Happy Blog" is no longer available.

https://cybersecuritynews.com/governments-hacked-revil-ransomware-group/

Click above link to read more.

Back to top

83% of ransomware victims paid the ransom to get their data restored – A shocking report

Almost two years after a wave of complaints flooded Google's support forums about YouTube accounts getting hijacked even if users had two-factor authentication enabled, Google's security team has finally tracked down the root cause of these attacks.

In a report published today, the Google Threat Analysis Group (TAG) attributed these incidents to "a group of hackers recruited in a Russian-speaking forum."

https://therecord.media/google-unmasks-two-year-old-phishing-malware-campaign-targeting-youtube-users/

Click above link to read more.

Back to top

Solarwinds hackers are targeting the global IT supply chain, Microsoft says

The Russian-linked hacking group that's been blamed for an attack on the U.S. government and a significant number of private U.S. companies last year is targeting key players in the global technology supply chain, according to cybersecurity experts at Microsoft.

Nobelium, as the hacking group is known, is infamous for the SolarWinds hack.

On Monday, Tom Burt, Microsoft corporate vice president of customer security and trust, said Nobelium has "been attempting to replicate the approach it has used in past attacks by targeting organizations integral to the global IT supply chain."

https://www.cnbc.com/2021/10/25/solarwinds-hackers-targeting-global-it-supply-chain-microsoft-says.html

Click above link to read more.

Back to top

Millions of Android users scammed in SMS fraud driven by Tik-Tok Ads

Threat actors are using malicious Android apps to scam users into signing up for a bogus premium SMS subscription service, which results in big charges accruing on their phone bills.

Jakub Vavra from the threat operations team of security firm Avast uncovered the campaign, which he dubbed UltimaSMS because one of the first apps he discovered being used to scam people was called Ultima Keyboard Pro, he said in a blog post published Monday.

https://threatpost.com/android-scammed-sms-fraud-tik-tok/175739/

Click above link to read more.

Back to top

---

7 ways to lock down enterprise printers

Following the PrintNightmare case, printer security has become a hot issue for security teams. Here are seven ways to keep printers secure on enterprise networks.

Enterprise printers have long been an afterthought in IT security, but all that changed earlier this year with PrintNightmare, a flaw in Microsoft's Windows Print Spooler Service that could be exploited in remote code execution attacks.

https://www.darkreading.com/edge-slideshows/7-ways-to-lock-down-enterprise-printers-

Click above link to read more.

Back to top

Google unmasks two-year-old phishing & malware campaign targeting YouTube users

Almost two years after a wave of complaints flooded Google's support forums about YouTube accounts getting hijacked even if users had two-factor authentication enabled, Google's security team has finally tracked down the root cause of these attacks.

In a report published today, the Google Threat Analysis Group (TAG) attributed these incidents to "a group of hackers recruited in a Russian-speaking forum."

https://therecord.media/google-unmasks-two-year-old-phishing-malware-campaign-targeting-youtube-users/

Click above link to read more.

Back to top

TeamTNT deploys malicious docker image on Docker Hub

Researchers at Uptycs Threat Research have uncovered a campaign in which the cloud-focused cryptojacking group TeamTNT is deploying malicious container images hosted on Docker Hub with an embedded script to download testing tools used for banner grabbing and port scanning.

Researchers identified the Zgrab scanner penetration testing tool, which is used for banner grabbing, and the masscanner penetration testing tool, which is used for port scanning.

https://www.bankinfosecurity.com/teamtnt-deploys-malicious-docker-image-on-docker-hub-a-17766

Click above link to read more.

Back to top

Nigerian romance scam targeted 100 women – FBI

Eight Nigerian men accused of an internet dating scam have appeared in a South African court after a massive international operation involving the FBI and Interpol.

Authorities in the US, where the investigation originated and most of the alleged victims are based, have applied for their extradition.

https://www.bbc.com/news/world-africa-58978287

Click above link to read more.

Back to top

Bug in popular WinRAR software could let attackers hack your computer

A new security weakness has been disclosed in the WinRAR trialware file archiver utility for Windows that could be abused by a remote attacker to execute arbitrary code on targeted systems, underscoring how vulnerabilities in such software could become a gateway for a roster of attacks.

Tracked as CVE-2021-35052, the bug impacts the trial version of the software running version 5.70. "This vulnerability allows an attacker to intercept and modify requests sent to the user of the application,"

Positive Technologies' Igor Sak-Sakovskiy said in a technical write-up. "This can be used to achieve remote code execution (RCE) on a victim's computer."

https://thehackernews.com/2021/10/bug-in-free-winrar-software-could-let.html

Click above link to read more.

Back to top

How do cyberattackers gain access to health systems? Often via smaller hospitals

Smaller hospitals are often how cyberattackers and nation states gain access to health system networks to steal IP, deploy ransomware or scour data to sell on the dark web, according to new research from cybersecurity firm CyCognito.

The firm's latest research studied health systems with more than $1 billion in revenue and more than 19 hospitals.

Healthcare IT News interviewed Rob Gurzeev, CEO and founder of CyCognito, to discuss the results of his firm's latest research, including why smaller hospitals are entry points for bad actors, how health systems are increasing risk by not paying their smaller entities enough attention, exactly how threat actors are using these points for entry, and how health systems can get a handle on extended attack surfaces.

https://www.healthcareitnews.com/news/how-do-cyberattackers-gain-access-health-systems-often-smaller-hospitals

Click above link to read more.

Back to top

TSA to issue cybersecurity requirements for US rail, aviation sectors

After issuing cybersecurity requirements for pipeline companies via two directives earlier this year, the Transportation Safety Administration (TSA) will now also issue cybersecurity requirements for rail systems and airport operators. The two pipeline directives followed a high-profile ransomware attack on Colonial Pipeline that shut off oil flow to the East Coast in May, sparking gas shortages and panic buying.

"TSA's broad responsibilities cover security at our airports, highways, and traffic management systems, pipelines, mass transit terminals and hubs, and subways and metros that carry billions of passengers every year," Department of Homeland Security (DHS) Secretary Alejandro Mayorkas said in announcing the new regulations yesterday. "Whether by air, land, or sea, our transportation systems are of utmost strategic importance to our national and economic security."

https://www.csoonline.com/article/3636408/tsa-to-issue-cybersecurity-requirements-for-us-rail-aviation-sectors.html

Click above link to read more.

Back to top

Attackers hijack craigslist emails to bypass security, deliver malware

Manipulated Craigslist emails that abuse Microsoft OneDrive warn users that their ads contain 'inappropriate content."

Musical instruments, motorcycle parts and now malware — Craigslist really does have it all.

The Craigslist internal email system was hijacked by attackers this month to deliver convincing messages messages, ultimately aimed avoiding Microsoft Office security controls to deliver malware.

https://threatpost.com/attackers-hijack-craigslist-email-malware/175754/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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