




December 22nd, 2020

Try our December - [“Shopping Online” Quiz](#)

This is the last digest for 2020

“Wishing you a safe and secure holiday season”

This week's stories:

- [Massive cyberattack grows beyond U.S., includes Canadian victims](#) 
- [FBI warns of ongoing COVID-19 vaccine related fraud schemes](#)
- [Zero-click iMessage zero-day used to hack the iPhones of 36 journalists](#)
- [Trucking giant Forward Air hit by new Hades ransomware gang](#)
- [Smart Doorbell Disaster: Many Brands Vulnerable to Attack](#)
- [Infosec pros warned of second SolarWinds Orion vulnerability](#)
- [Dark Web Pricing Skyrockets for Microsoft RDP Servers, Payment-Card Data](#)

Massive cyberattack grows beyond U.S., includes Canadian victims 

<https://www.ctvnews.ca/sci-tech/massive-cyberattack-grows-beyond-u-s-includes-canadian-victims-1.5237313>

WASHINGTON -- A devastating cyberattack on U.S. government agencies has also hit targets worldwide with the list of victims still growing, according to researchers, heightening fears over computer security and espionage.

Microsoft said late Thursday that it had notified more than 40 customers hit by the malware which security experts say came from hackers linked to the Russian government and which could allow attackers unfettered network access.

[Click link above to read more](#)

FBI warns of ongoing COVID-19 vaccine related fraud schemes

<https://www.bleepingcomputer.com/news/security/fbi-warns-of-ongoing-covid-19-vaccine-related-fraud-schemes/>

US federal agencies have warned about scammers exploiting the public's interest in the COVID-19 vaccine to harvest personal information and steal money through multiple ongoing and emerging fraud schemes.

The warning was issued earlier today through the FBI National Press Office by the Federal Bureau of Investigation (FBI), the Department of Health and Human Services Office of Inspector General (HHS-OIG), and the Centers for Medicare & Medicaid Services (CMS).

[Click link above to read more](#)

Zero-click iMessage zero-day used to hack the iPhones of 36 journalists

<https://arstechnica.com/information-technology/2020/12/zero-click-imessage-zero-day-used-to-hack-the-iphones-of-36-journalists/>

Three dozen journalists had their iPhones hacked in July and August using what at the time was an iMessage zero-day exploit that didn't require the victims to take any action to be infected, researchers said.

The exploit and the payload it installed were developed and sold by NSO Group, according to a report published Sunday by Citizen Lab, a group at the University of Toronto that researches and exposes hacks on dissidents and journalists. NSO is a maker of offensive hacking tools that has come under fire over the past few years for selling its products to groups and governments with poor human rights records. NSO has disputed some of the conclusions in the Citizen Lab report.

[Click link above to read more](#)

Trucking giant Forward Air hit by new Hades ransomware gang

<https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-hit-by-new-hades-ransomware-gang/>

Trucking and freight logistics company Forward Air has suffered a ransomware attack by a new ransomware gang that has impacted the company's business operations.

Forward Air is a leading trucking and air freight logistics company based out of Tennessee, USA. The company generated \$1.4 billion in revenue for 2019 and employs over 4,300 people.

[Click link above to read more](#)

Smart Doorbell Disaster: Many Brands Vulnerable to Attack

<https://threatpost.com/smart-doorbell-vulnerable-to-attack/162527/>

Investigation reveals device sector is problem plagued when it comes to security bugs.

Smart doorbells, designed to allow homeowners to keep an eye on unwanted and wanted visitors, can often cause more security harm than good compared to their analog door bolt alternatives. Consumer-grade digital doorbells are riddled with potential cybersecurity vulnerabilities ranging from hardcoded credentials, authentication issues and devices shipping with unpatched and longstanding critical bugs.

[Click link above to read more](#)

Infosec pros warned of second SolarWinds Orion vulnerability

<https://www.itworldcanada.com/article/infosec-pros-warned-of-second-solarwinds-orion-vulnerability/439971>

IT administrators that use SolarWinds' Orion network management platform have more than one vulnerability to search for in the wake of news the suite has been compromised.

Dubbed Supernova by Palo Alto Networks, it's described as a "sophisticated, in-memory webshell baked into Orion's code, which acted as an interactive .NET runtime API." The webshell payload is compiled on

the fly and executed dynamically, the report says, which makes it less easy to detect by endpoint detection applications.

[Click link above to read more](#)

Dark Web Pricing Skyrockets for Microsoft RDP Servers, Payment-Card Data

<https://threatpost.com/rdp-server-access-payment-card-data-in-high-cybercrime-demand/162476/>

Underground marketplace pricing on RDP server access, compromised payment card data and DDoS-For-Hire services are surging.

Cybercriminals are vying for Remote Desktop Protocol (RDP) access, stolen payment cards and DDoS-for-Hire services, based on a recent analysis of underground marketplace pricing.

During the COVID-19 pandemic, cybercriminals have profited with “increasingly advantageous positions to benefit from the disruption,” said researchers — and this has also been reflected on underground markets, where new services like targeted ransomware and advanced SIM swapping are popping up.

[Click link above to read more](#)

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.

