Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

September 28, 2021

Challenge yourself with our ABCs of Cyber Security quiz!

Join Cyber Security Awareness Month!

Register for Security Day

This week's stories:

🍁 Canadian firm VoIP.ms hit by non-stop extortion-based DDoS attacks

A new bug in Microsoft Windows could let hackers easily install a rootkit

Ransomware attacks on coops may just be the start of ag sector security woes

REvil ransomware group's latest victim: Its own affiliates

A new Jupyter malware version is being distributed via MSI installers

New security tech enables 75% cost avoidance for Oregon radiologists

Autodiscover flaw in Microsoft Exchange leaking credentials

Critical Cisco bugs allow code execution on wireless, SD-WAN

APT actors exploit flaw in ManageEngine single sign-on solution

Seven strategies for building a great security team

Major European call center provider goes down in ransomware attack

New BloodyStealer trojan steals gamers' Epic Games and Steam accounts

---

Canadian firm VoIP.ms hit by non-stop extortion-based DDoS attacks

A Quebec-based Internet phone service provider VoIP.ms, which offers voice-over-IP services, has been down since September 17th. Reportedly, the firm is being held to ransom after becoming a victim of a massive and sustained DDoS attack. The assault has severely disrupted its operations.

According to VoIP.ms, the attacks started on September 16th, targeting their DNS name servers and other infrastructure, disrupting their telephony services due to which people couldn't make or receive calls.

https://www.hackread.com/canadian-voip-ms-hit-by-extortion-ddos-attacks/

Click above link to read more.

Back to top

A new bug in Microsoft Windows could let hackers easily install a rootkit

Security researchers have disclosed an unpatched weakness in Microsoft Windows Platform Binary Table (WPBT) affecting all Windows-based devices since Windows 8 that could be potentially exploited to install a rootkit and compromise the integrity of devices.

"These flaws make every Windows system vulnerable to easily-crafted attacks that install fraudulent vendor-specific tables," researchers from Eclypsium said in a report published on Monday. "These tables can be exploited by attackers with direct physical access, with remote access, or through manufacturer supply chains. More importantly, these motherboard-level flaws can obviate initiatives like Secured-core because of the ubiquitous usage of ACPI [Advanced Configuration and Power Interface] and WPBT."

https://thehackernews.com/2021/09/a-new-bug-in-microsoft-windows-could.html

Click above link to read more.

Back to top

Ransomware attacks on coops may just be the start of ag security sector woes

Recent ransomware attacks against U.S. grain cooperatives and a farm data platform are raising the specter of food supply chain disruptions while highlighting the economic and physical security risks of reliance on increasingly sophisticated systems to feed the world.

America’s farms have led the way in real-world applications of innovations, from self-driving vehicles to satellite imagery, so much so that many farmers are already living in the future: They rely on farm platforms that can connect information from their tractors, drones, satellites, soil samples, and public sources to map out plans for planting, which herbicides or pesticides to use, and harvests.

https://therecord.media/ransomware-attacks-on-grain-coops-may-just-be-the-start-of-ag-sector-security-woes/

Click above link to read more.

Back to top

REvil ransomware group’s latest victim: Its own affiliates

Ransomware-wielding attackers love to lie.

Of course they never knowingly hit the healthcare sector or other so-called critical infrastructure. If they say they've stolen data, without a doubt they really stole data.

https://www.bankinfosecurity.com/blogs/revil-ransomware-groups-latest-victim-its-own-affiliates-p-3125

Click above link to read more.

Back to top

A new Jupyter malware version is being distributed via MSI installers

Cybersecurity researchers have charted the evolution of Jupyter, a .NET infostealer known for singling out healthcare and education sectors, which make it exceptional at defeating most endpoint security scanning solutions.

The new delivery chain, spotted by Morphisec on September 8, underscores that the malware has not just continued to remain active but also showcases "how threat actors continue to develop their attacks to become more efficient and evasive." The Israeli company said it's currently investigating the scale and scope of the attacks.

https://thehackernews.com/2021/09/a-new-jupyter-malware-version-is-being.html

Click above link to read more.

Back to top

New security tech enables 75% cost avoidance for Oregon radiologists

At Central Oregon Radiology Associates, network detection and response technology provides improved, more manageable security while cutting costs, its CIO reports.

Central Oregon Radiology Associates, Cascade Medical Imaging and Central Oregon Magnetic Resonance Imaging collectively exist to provide the full scope of quality diagnostic imaging services to the Central and Eastern Oregon communities.

https://www.healthcareitnews.com/news/new-security-tech-enables-75-cost-avoidance-oregon-radiologists

Click above link to read more.

Back to top

Autodiscover flaw in Microsoft Exchange leaking credentials

A flaw in Autodiscover, a protocol utilized in Microsoft Exchange, is responsible for a massive data leak of various Windows and Microsoft credentials, according to new Guardicore research.

Autodiscover is used by Exchange to automatically configure client applications like Microsoft Outlook. In research published Wednesday, Amit Serper, area vice president of security research for enterprise security vendor Guardicore, wrote in the company's post dedicated to the vulnerability that Autodiscover "has a design flaw that causes the protocol to 'leak' web requests to Autodiscover domains outside of the user's domain," but in the same top-level domain (TLD) -- for example, Autodiscover.com.

https://searchsecurity.techtarget.com/news/252507119/Autodiscover-flaw-in-Microsoft-Exchange-leaking-credentials

Click above link to read more.

Back to top

Critical Cisco bugs allow code execution on wireless, SD-WAN

Cisco is warning three critical security vulnerabilities affect its flagship IOS XE software, the operating system for most of its enterprise networking portfolio. The flaws impact Cisco’s wireless controllers, SD-WAN offering and configuration mechanisms in use for scads of products.

The networking giant has released patches for all of them, as part of a comprehensive 32-bug update released this week.

https://threatpost.com/critical-cisco-bugs-wireless-sd-wan/174991/

Click above link to read more.

Back to top

APT actors exploit flaw in ManageEngine single sign-on solution

Cyberespionage groups are exploiting a critical vulnerability patched earlier this month in ManageEngine ADSelfService Plus, a self-service password management and single sign-on (SSO) solution for Active Directory environments. The FBI, CISA and the United States Coast Guard Cyber Command (CGCYBER) urge organizations who use the product to deploy the available patch as soon as possible and check their systems for signs of compromise.

"The FBI, CISA, and CGCYBER assess that advanced persistent threat (APT) cyber actors are likely among those exploiting the vulnerability," the three agencies said in a joint advisory. "The exploitation of ManageEngine ADSelfService Plus poses a serious risk to critical infrastructure companies, US-cleared defense contractors, academic institutions, and other entities that use the software."

https://www.csoonline.com/article/3633644/apt-actors-exploit-flaw-in-manageengine-single-sign-on-solution.html

Click above link to read more.

Back to top

Seven strategies for building a great security team

Brennan P. Baybeck lists building a successful team as one of his top responsibilities as a CISO.

“If you surround yourself with great people, make sure they’re successful and have what they need—the training, the budget, the right headcount—then great security comes along,” he says. “But if you don’t put that focus on your team, it’s not going to happen.

https://www.csoonline.com/article/3633595/seven-strategies-for-building-a-great-security-team.html

Click above link to read more.

Back to top

Major European call center provider goes down in ransomware attack

GSS, the Spanish and Latin America division of Covisian, one of Europe’s largest customer care and call center providers, has suffered a debilitating ransomware attack that froze a large part of its IT systems and crippled call centers across its Spanish-speaking customer base.

Call centers and automated customer support phone services for companies and government organizations in Spain and Latin America have been unreachable this week.

https://therecord.media/major-european-call-center-provider-goes-down-in-ransomware-attack/

Click above link to read more.

Back to top

New BloodyStealer trojan steals gamers' Epic Games and Steam accounts

A new advanced trojan sold on Russian-speaking underground forums comes with capabilities to steal users' accounts on popular online video game distribution services, including Steam, Epic Games Store, and EA Origin, underscoring a growing threat to the lucrative gaming market.

Cybersecurity firm Kaspersky, which coined the malware "BloodyStealer," said it first detected the malicious tool in March 2021 as being advertised for sale at an attractive price of 700 RUB (less than $10) for one month or $40 for a lifetime subscription. Attacks using Bloody Stealer have been uncovered so far in Europe, Latin America, and the Asia-Pacific region.

https://thehackernews.com/2021/09/new-bloodystealer-trojan-steals-gamers.html

Click above link to read more.

Back to top

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

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.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer