August 3, 2021

Challenge yourself with our NEW Safe Surfing quiz!

Multi-Factor Authentication is currently rolling out across the BC Government now through October. Check your inbox regularly for an MFA registration email.

This week's stories:

Canadian VPN provider Windscribe admits seized Ukrainian servers weren't encrypted

CISA launches new vulnerability disclosure policy platform

Top 30 most targeted vulnerabilities for the last 2 years – FBI

New Android malware records smartphones via VNC to steal passwords

NSA warns public networks are hacker hotbeds

Novel meteor wiper used in attack that crippled Iranian train system

Phony call centers tricking users into installing ransomware and data-stealers

Hackers exploit Microsoft browser bug to deploy VBA malware on targeted PCs

Windows PetitPotam attacks can be blocked using new method

Lower-level employees become top spear-phishing targets

Canadian VPN provider Windscribe admits seized Ukrainian servers weren't encrypted

Windscribe, a Canadian-based VPN provider, says it realized two of its servers that were seized last year by Ukrainian authorities were unencrypted, leaving open the possibility that, at least temporarily, someone could have accessed traffic.

Since discovering the incident earlier this month the company has been overhauling its infrastructure to improve security.

https://www.itworldcanada.com/article/canadian-vpn-provider-windscribe-admits-seized-ukrainian-servers-werent-encrypted/456507

Click above link to read more.

Back to top

CISA launches new vulnerability disclosure policy platform

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has debuted its vulnerability disclosure policy (VDP) platform for the federal civilian enterprise.

Its launch of the VDP follows last fall's release of the Binding Operational Directive (BOD 20-01), issued in support of the Office of Management and Budget's M-20-32, "Improving Vulnerability Identification, Management, and Remediation." BOD 20-01 requires agencies to establish policies that enable the public to contribute and report vulnerability disclosures.

https://www.darkreading.com/vulnerabilities-threats/cisa-launches-new-vulnerability-disclosure-policy-platform

Click above link to read more.

Back to top

Top 30 most targeted vulnerabilities for the last 2 years – FBI

Each and every year in the software and hardware that we use every day thousands of vulnerabilities are discovered by security researchers.

However, now the FBI and the CISA have taken a step further to reveal the most targeted vulnerabilities for the last 2 years, as this will help the security researchers and security organizations to patch the vulnerabilities that were not fixed yet.

https://cybersecuritynews.com/top-30-most-targeted-vulnerabilities/

Click above link to read more.

Back to top

New Android malware records smartphones via VNC to steal passwords

Security researchers have discovered a novel piece of Android malware that uses the VNC technology to record and broadcast a victim’s smartphone activity, allowing threat actors to collect keyboard presses and app passwords.

First spotted in March 2021 by Dutch security firm ThreatFabric, this new piece of malware, named Vultur, is a departure from other Android malware strains that usually rely on fake login screens floating on top of legitimate apps to collect a victim’s credentials.

https://therecord.media/new-android-malware-records-smartphones-via-vnc-to-steal-passwords/

Click above link to read more.

Back to top

NSA warns public networks are hacker hotbeds

Agency warns attackers targeting teleworkers to steal corporate data.

The U.S. National Security Agency is offering advice to security teams looking for wireless best practices to protect corporate networks and personal devices. The recommendations, while pedestrian in scope, do offer system administrators a solid cheat sheet to share with their work-from-home crowd and mobile workforces.

https://threatpost.com/nsa-warns-public-networks-are-hacker-hotbeds/168268/

Click above link to read more.

Back to top

Novel meteor wiper used in attack that crippled Iranian train system

A July 9th attack disrupted service and taunted Iran's leadership with hacked screens directing customers to call the phone of Iranian Supreme Leader Khamenei with complaints.

An attack earlier this month on Iran's train system, which disrupted rail service and taunted Iran's leadership via hacked public transit display screens, used a never-before-seen wiper malware called Meteor that appears to have been design for reuse, a security researcher has found.

https://threatpost.com/novel-meteor-wiper-used-in-attack-that-crippled-iranian-train-system/168262/

Click above link to read more.

Back to top

Phony call centers tricking users into installing ransomware and data-stealers

An ongoing malicious campaign that employs phony call centers has been found to trick victims into downloading malware capable of data exfiltration as well as deploying ransomware on infected systems.

The attacks — dubbed "BazaCall" — eschew traditional social engineering techniques that rely on rogue URLs and malware-laced documents in favor of a vishing-like method wherein targeted users are sent email messages informing them of a forthcoming subscription charge unless they call a specific phone number.

https://thehackernews.com/2021/07/phony-call-centers-tricking-users-into.html

Click above link to read more.

Back to top

Hackers exploit Microsoft browser bug to deploy VBA malware on targeted PCs

An unidentified threat actor has been exploiting a now-patched zero-day flaw in Internet Explorer browser to deliver a fully-featured VBA-based remote access trojan (RAT) capable of accessing files stored in compromised Windows systems, and downloading and executing malicious payloads as part of an "unusual" campaign.

The backdoor is distributed via a decoy document named "Manifest.docx" that loads the exploit code for the vulnerability from an embedded template, which, in turn, executes shellcode to deploy the RAT, according to cybersecurity firm Malwarebytes, which spotted the suspicious Word file on July 21, 2021.

https://thehackernews.com/2021/07/hackers-exploit-microsoft-browser-bug.html

Click above link to read more.

Back to top

Windows PetitPotam attacks can be blocked using new method

Security researchers have devised a way to block the recently disclosed PetitPotam attack vector that allows hackers to take control of a Windows domain controller easily.

Last month, security researcher GILLES Lionel disclosed a new method called PetitPotam that forces a Windows machine, including a Windows domain controller, to authenticate against a threat actor's malicious NTLM relay server using the Microsoft Encrypting File System Remote Protocol (EFSRPC).

Threat actors would then relay this authentication request to a targeted domain's Active Directory Certificate Services via HTTP., where the attacker would be given a Kerberos ticket-granting ticket (TGT), allowing them to assume the domain controller's identity.

https://www.bleepingcomputer.com/news/microsoft/windows-petitpotam-attacks-can-be-blocked-using-new-method/

Click above link to read more.

Back to top

Lower-level employees become top spear-phishing targets

The average organization is targeted by over 700 social engineering attacks each year, according to a new report that reveals current trends in phishing and spearphishing.

Between May 2020 and June 2021, researchers with security firm Barracuda analyzed more than 12 million spearphishing and social engineering attacks related to 3 million mailboxes at more than 17,000 organizations. Results reveal some of the common methods attackers use to breach victims' defenses, such as trying to exploit a widespread interest in cryptocurrency and tailoring attacks to target less suspicious employees in low-profile roles.

https://www.darkreading.com/attacks-breaches/lower-level-employees-become-top-spearphishing-targets

Click above link to read more.

Back to top

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