May 4, 2021

Challenge yourself with our Spotting a Fake quiz!

This week's stories:

B.C.'s student aid one of 'multiple government websites' down, reports of possible hacking shared

Whistler the latest Canadian municipality hit by ransomware attack

Bell launches BSURE managed cybersecurity solutions with Fortinet

Hackers Use SMS Phishing Scams to Trick Rogers Customers with Outage Refunds

These breached "Star Wars"-themed passwords need more than the force to save them

Why can't Google get a grip on rip-off ads?

Researchers Uncover Iranian State-Sponsored Ransomware Operation

Fortnite-maker Epic Games challenges Apple's 'walled garden' app store in court

DDoS attackers stick to their target even if they are unsuccessful

Swiss Cloud becomes the latest web hosting provider to suffer a ransomware attack

PHP package manager flaw left millions of web apps open to abuse

Pulse Secure releases patch for zero-day used to target defense firms

Over 40 Apps With More Than 100 Million Installs Found Leaking AWS Keys

Apple hurries out fixes for WebKit zero-days

New Phishing Campaign Found in (SEG) Uses SharePoint Documents

Deepfake Attacks Are About to Surge, Experts Warn

The ransomware surge ruining lives

B.C.'s student aid one of 'multiple government websites' down, reports of possible hacking shared

VANCOUVER -- A website that manages post-secondary student loans in B.C. is offline, with reports on social media suggesting the site may have been hacked.

StudentAid BC posted to Twitter just before 9 a.m. Monday saying its website "is temporarily down" and the team is working to "resolve an issue affecting multiple government websites."

The agency didn't provide details on why the website was down, but some people on social media had a theory and shared pictures of what the site reportedly looked like on Sunday.

Those images show a black screen with a green logo and the name "Guardiran Security Team." A phrase underneath says, "Mess with the best, die like the rest.".

https://bc.ctvnews.ca/b-c-s-student-aid-one-of-multiple-government-websites-down-reports-of-possible-hacking-shared-1.5411974

Click link above to read more

Whistler the latest Canadian municipality hit by ransomware attack

One of the country's foremost ski resorts is struggling to dig itself out from a ransomware attack.

The Resort Municipality of Whistler (RMOW), just over an hour's drive north of Vancouver, suffered what it calls a cybersecurity event on Thursday. As a result, non-essential town services have been suspended because email, phone, network services and the website were taken offline.

In-person service at the municipal hall is suspended and the May 4 town council meeting has been cancelled.

https://www.itworldcanada.com/article/whistler-the-latest-canadian-municipality-hit-by-ransomware-attack/446752.

Click link above to read more

Bell launches BSURE managed cybersecurity solutions with Fortinet

Designed for cloud, IoT and upcoming networking technologies, BSURE combines Bell's national Security Operations Centre with Fortinet's security information and event management, as well as its security orchestration, automation and response technologies. The management system can prioritize alerts on the customer's behalf and address the most impactful threats first.

The new service complements Bell's existing cybersecurity solutions, including firewall services, VPN, and authentications. The company also pulls security insights from various security organizations, including the government.

"Combining these key capabilities in our BSURE solution is a big win for Canadian organizations seeking to enhance control of their security operations in a transforming digital economy," said Jeremy Wubs, senior vice-president of marketing for Bell Business Markets, in the news release. "BSURE offers our customers an integrated, automated and fully managed solution that reduces risk to their infrastructure and critical data and the complexities of cybersecurity management.".

https://www.itworldcanada.com/article/bell-launches-bsure-managed-cybersecurity-solutions-with-fortinet/446904

Click link above to read more

Hackers Use SMS Phishing Scams to Trick Rogers Customers with Outage Refunds

Rogers Communications Inc. is warning Canadians to keep an eye out for SMS phishing scams offering to reimburse customers for the system outage earlier last week.

Users were blocked from accessing wireless voice and data services after the company suffered an outage throughout Canada a week ago. Now threat actors are sending malicious text messages asking recipients to click on a link to claim their rebate.

An SMS posted on social media fakely claims that "R0GERS WIRELESS INC." (spelled with a zero instead of the letter O) is offering a $50 credit if people click on a provided link.

https://heimdalsecurity.com/blog/hackers-use-sms-phishing-scams-to-trick-rogers-customers/

Click link above to read more

These breached "Star Wars"-themed passwords need more than the force to save them

Due to its phonetic similarities with the famous line in the storied film franchise —"May the force be with you"—May 4 is also known as Star Wars Day among sci-fans and cinephiles alike. Just in time for the occasion, Specops Software, a password management and authentication company, released a roundup of the most commonly used "Star Wars"-themed passwords. Turns out, even the most sci-fi-inspired passwords still need the occasional capital letter and special character splashed in.

"'Star Wars' fans might wish they could use the Force to stop password attacks but sadly that option is unavailable to us," said Darren James, head of internal IT at Specops Software.

"Password attacks continue to rise and the only real solution is to ensure you have secure password policies in place to protect your network, especially policies that protect against the use of leaked passwords," James continued.

https://www.techrepublic.com/article/these-breached-star-wars-themed-passwords-need-more-than-the-force-to-save-them/

Click link above to read more

Why can't Google get a grip on rip-off ads?

Google has failed to stop "shyster" websites advertising on its search engine, despite promising to fix the problem, the BBC has found.

Adverts for unofficial services selling government documents such as travel permits and driving licences are against Google's own rules.

But the BBC found adverts for expensive third-party sellers every time it searched during a 12-month period.

In a statement Google said it had taken down billions of rule-breaking adverts.

What is the issue?

In the UK, changing the address on your driving licence is free - but Google consistently showed adverts for services charging £49.99.

Applying for an Esta travel permit to visit the US should cost no more $14 (£10) - but Google repeatedly allowed adverts for websites charging more than $80.

In Google's search results, adverts look similar to organic results and appear at the top of the list.

https://www.bbc.com/news/technology-56886957

Click link above to read more

Researchers Uncover Iranian State-Sponsored Ransomware Operation

Iran has been linked to yet another state-sponsored ransomware operation through a contracting company based in the country, according to new analysis.

"Iran's Islamic Revolutionary Guard Corps (IRGC) was operating a state-sponsored ransomware campaign through an Iranian contracting company called 'Emen Net Pasargard' (ENP)," cybersecurity firm Flashpoint said in its findings summarizing three documents leaked by an anonymous entity named Read My Lips or Lab Dookhtegan between March 19 and April 1 via its Telegram channel.

Dubbed "Project Signal," the initiative is said to have kickstarted sometime between late July 2020 and early September 2020, with ENP's internal research organization, named the "Studies Center," putting together a list of unspecified target websites.

https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html

Click link above to read more

Fortnite-maker Epic Games challenges Apple's 'walled garden' app store in court

On Monday, Apple faces one of its most serious legal threats in recent years: A trial that threatens to upend its iron control over its app store, which brings in billions of dollars each year while feeding more than 1.6 billion iPhones, iPads, and other devices.

The federal court case is being brought by Epic Games, maker of the popular video game Fortnite. Epic wants to topple the so-called "walled garden" of the app store, which Apple started building 13 years ago as part of a strategy masterminded by co-founder Steve Jobs.

Epic charges that Apple has transformed a once-tiny digital storefront into an illegal monopoly that squeezes mobile apps for a significant slice of their earnings. Apple takes a commission of 15% to 30% on purchases made within apps, including everything from digital items in games to subscriptions. Apple denies Epic's claims.

https://www.ctvnews.ca/sci-tech/fortnite-maker-epic-games-and-apple-get-their-day-in-court-app-store-commissions-at-stake-1.5411442

Click link above to read more

DDoS attackers stick to their target even if they are unsuccessful

Between January and March, more than double the number of attacks than the same period in the previous year were recorded. This suggest the already alarming threat level from cybercrime, a pandemic that has been raging since Spring 2020 alongside the fight against COVID-19, has once again intensified.

DDoS attackers stick to their target

- The number of attacks continued to increase: 128% increase in the number of attacks than Q1 2020 (factor of around 2.3).
- Attack bandwidths remained high: 216 Gbps maximum in attack volume.
- Increasing use of carpet-bombing attacks: Attackers are more and more switching to carpet bombing attacks with small-volume, low-threshold attacks, which remain under the radar of many protection solutions. The hundreds or thousands of small attacks running in parallel can easily add up to a high-volume attack of several tens or hundreds of Gbps and cause an infrastructure to collapse. This is particularly worrisome for hosting and cloud providers.
- Highly dynamic attack tactics: 69% of attacks were multi-vector attacks combining multiple techniques.
- DDoS attackers stick to their target even if they are unsuccessful: 1489 minutes was the longest attack (>24 h). Without effective protection, long recovery times, which can be twice or three times as long as the actual attack, would still have to be considered.

https://www.helpnetsecurity.com/2021/05/03/ddos-attackers-stick-to-their-target/

Click link above to read more

Swiss Cloud becomes the latest web hosting provider to suffer a ransomware attack

Swiss Cloud, a Switzerland-based cloud hosting provider, has suffered this week a ransomware attack that brought the company’s server infrastructure to its knees.

The incident took place on Tuesday, April 27, according to Swiss Cloud’s status page.

The company, which is one of Switzerland’s largest hosting providers, said on Friday in an update posted on its website that it’s working to restore affected servers from existing backups.

The process is expected to take at least a few days. Swiss Cloud said its staff is working in 24-hour shifts, including over the weekend, to restore services as early as next week.

Experts from HPE and Microsoft are also helping with the process, the company said.

It is currently unknown which ransomware gang targeted Swiss Cloud and what’s the size of their ransom demand. A Swiss Cloud spokesperson did not return a request for comment.

https://therecord.media/swiss-cloud-becomes-the-latest-web-hosting-provider-to-suffer-a-ransomware-attack/

Click link above to read more

PHP package manager flaw left millions of web apps open to abuse

Security researchers are warning that a software supply chain vulnerability impacting PHP could put millions of websites at risk.

The flaw, discovered by security researchers at SonarSource, affects Composer, the main tool used to manage and install dependencies for PHP.

Composer itself uses Packagist, an online service for managing PHP package requests, which is where the flaw was found.

SonarSource discovered a vulnerability allowing attackers to execute arbitrary system commands on the Packagist server. This could be used to obtain maintainers' credentials, or to redirect package requests.

"An attacker changing the URL associated with the package symfony/symfony by one under their control would trick Composer into downloading the wrong source code, and with that deploy the attacker's backdoor on the server running Composer," Thomas Chauchefoin, vulnerability researcher at SonarSource told The Daily Swig.

https://portswigger.net/daily-swig/php-package-manager-flaw-left-millions-of-web-apps-open-to-abuse

Click link above to read more

Pulse Secure releases patch for zero-day used to target defense firms

Pulse Secure on Monday released a patch for the zero-day vulnerability that hackers used to access the networks of U.S. defense contractors and other government agencies worldwide.

In a blog posted April 20, FireEye said Chinese-based UNC2630 leveraged CVE-2021-22893 to gain access to Pulse Secure VPN equiptment and move laterally. A second threat actor, UNC2717, was also identified exploiting Pulse Secure VPN equipment, but FireEye could not connect them to UNC2630.

Pulse Security said over the past couple of weeks it has worked closely with the Cybersecurity and Infrastructure Security Agency (CISA) as well as FireEye and Stroz Friedberg to investigate and respond quickly to the malicious activity that was identified on its customers' systems.

FireEye said it observed UNC2630 harvesting credentials from various Pulse Secure VPN login flows, which ultimately led the bad threat actor to use legitimate account credentials to move laterally into defense industrial base (DIB) companies.

https://www.scmagazine.com/home/security-news/government-and-defense/pulse-secure-releases-patch-for-zero-day-used-to-target-defense-industrial-base/

Click link above to read more

Over 40 Apps With More Than 100 Million Installs Found Leaking AWS Keys

Most mobile app users tend to blindly trust that the apps they download from app stores are safe and secure. But that isn't always the case.

To demonstrate the pitfalls and identify vulnerabilities on a large scale, cybersecurity and machine intelligence company CloudSEK recently provided a platform called BeVigil where individuals can search and check app security ratings and other security issues before installing an app.

A latest report shared with The Hacker News detailed how the BeVigil search engine identified over 40 apps - with more than a cumulative 100 million downloads - that had hardcoded private Amazon Web Services (AWS) keys embedded within them, putting their internal networks and their users' data at risk of cyberattacks.

https://thehackernews.com/2021/05/over-40-apps-with-more-than-100-million.html

Click link above to read more

Apple hurries out fixes for WebKit zero-days

Apple dropped updates on Monday for iOS, macOS, and watchOS in response to in-the-wild attacks on its WebKit browser engine.

The macOS Big Sur 11.3.1, iOS/iPadOS 14.5.1, and iOS 12.5.3 each include fixes for CVE-2021-30665 and CVE-2021-30663. Both flaws are present in WebKit, the engine Apple uses as the basis for its Safari desktop browser and multiple components of iOS.

Each of the two bugs allow for an attacker to run arbitrary code and commands by way of a poisoned web page. In the case of CVE-2021-30665, discovered by a trio of researchers with Chinese security vendor Qihoo 360 ATA, the exploit is carried out by way of a memory corruption error that allows code injection. CVE-2021-30663, which was discovered by an anonymous researcher, was blamed on an integer overflow error caused by improper handling of user input.

https://searchsecurity.techtarget.com/news/252500162/Apple-hurries-out-fixes-for-WebKit-zero-days

Click link above to read more

New Phishing Campaign Found in (SEG) Uses SharePoint Documents

The Cofense Phishing Defense Center (PDC) has revealed a phishing campaign that targets Office 365 users and includes a convincing SharePoint document claiming to urgently need an email signature.

This new phishing campaign found in an environment protected by Microsoft's secure email gateway (SEG). Since thousands of individuals still required to telework, hackers lure their victims with almost picture-perfect sharing themed emails.

(IMAGE)

The above Email showcases correct spelling and grammar in messaging that include urgency ("and response urgently"). The user's name is not clear in the opening message above, indicating that this is a mass-distribution campaign intended to reach multiple users.

https://cybersecuritynews.com/phishing-campaign-sharepoint-documents/

Click link above to read more

Deepfake Attacks Are About to Surge, Experts Warn

New deepfake products and services are cropping up across the Dark Web.

Artificial intelligence and the rise of deepfake technology is something cybersecurity researchers have cautioned about for years and now it's officially arrived. Cybercriminals are increasingly sharing, developing and deploying deepfake technologies to bypass biometric security protections, and in crimes including blackmail, identity theft, social engineering-based attacks and more, experts warn.

Time to get those cybersecurity defenses ready.

A drastic uptick in deepfake technology and service offerings across the Dark Web is the first sign a new wave of fraud is just about to crash in, according to a new report from Recorded Future, which ominously predicted that deepfakes are on the rise among threat actors with an enormous range of goals and interests.

"Within the next few years, both criminal and nation-state threat actors involved in disinformation and influence operations will likely gravitate towards deepfakes, as online media consumption shifts more into 'seeing is believing' and the bet that a proportion of the online community will continue to be susceptible to false or misleading information," the Recorded Future report said.

https://threatpost.com/deepfake-attacks-surge-experts-warn/165798/

Click link above to read more

The ransomware surge ruining lives

A global coalition of technology companies and law enforcement bodies is calling for "aggressive and urgent" action against ransomware.

Microsoft, Amazon, the FBI and the UK's National Crime Agency have joined the Ransomware Task Force (RTF) in giving governments nearly 50 recommendations.

Ransomware gangs are now routinely targeting schools and hospitals.

Hackers use malicious software to scramble and steal an organisation's computer data.

The RTF has submitted its report to President Biden's administration.

It argues that "more than just money is at stake" and says that, in just a few years, "ransomware has become a serious national security threat and public health and safety concern".

https://www.bbc.com/news/technology-56933733

Click link above to read more