July 13, 2021

Challenge yourself with our Password Security quiz!

This week's stories:

Cybersecurity insurance rates likely to rise amid escalated ransomware attacks

Companies looking to purchase insurance against cyberattacks in which their data is held for ransom will soon find it more expensive and difficult to obtain, a cybersecurity expert says.

Brent Arnold, a partner at law firm Gowlings WLG in Toronto, says the U.S. insurance industry has already tightened its requirements for providing coverage for criminal ransomware attacks.

https://www.canadiansecuritymag.com/cybersecurity-insurance-rates-likely-to-rise-amid-escalating-ransomware-attacks/

Click above link to read more.

Back to top

Kaseya releases security patch as companies continue to recover

Kaseya, provider of remote management and monitoring software, released a patch on July 11 to fix a vulnerability in its server that the Russia-linked REvil group exploited nine days earlier to launch a ransomware attack against managed service providers and their clients.

While 95% of its cloud-based customers have been returned to service, the attack continues to affect Kaseya customers and clients. Some companies continue to struggle as others have begun returning to some semblance of normal business.

https://www.darkreading.com/attacks-breaches/kaseya-releases-security-patch-as-companies-continue-to-recover/d/d-id/1341514

Click above link to read more.

Back to top

SolarWinds issues hotfix for zero-day flaw under active attack

Microsoft alerted the company to a security vulnerability in its Serv-U Managed File Transfer and Secure FTP products that a cyberattacker is using to target a “limited” amount of customers.

SolarWinds has issued a hotfix for a zero-day remote code execution (RCE) vulnerability already under active, yet limited, attack on some of the company’s customers.

https://threatpost.com/solarwinds-hotfix-zero-day-active-attack/167704/

Click above link to read more.

Back to top

Microsoft releases emergency patch for 'PrintNightmare' vuln

Microsoft has rushed out an emergency security update for "PrintNightmare," a critical remote code execution vulnerability present in all versions of its Windows operating system.

In an advisory Tuesday afternoon, the company urged organizations to apply the patches immediately, saying it had detected active exploitation of the bug. For enterprises that are unable to patch immediately, Microsoft recommended they implement several workarounds and mitigations it had released a day earlier.

https://www.darkreading.com/endpoint/microsoft-releases-emergency-patch-for-printnightmare-vuln/d/d-id/1341493

Click above link to read more.

Back to top

Kaseya hacked via authentication bypass

The Kaseya ransomware attack is believed to have been down to an authentication bypass. Yes, ransomware needs to be on your radar -- but good authentication practices are also imperative.

Last Friday, just before the extended American Independence Day holiday, it was announced that Kaseya, an American software company, was hacked. The malicious actors were able to distribute ransomware by exploiting several vulnerabilities in Kaseya's Vector Signal Analysis (VSA) software, which gave the attackers the ability to infect multiple organizations via what is known as a supply chain attack.

https://beta.darkreading.com/omdia/kaseya-hacked-via-authentication-bypass

Click above link to read more.

Back to top

Kaseya raced to patch before ransomware disaster

Global software vendor Kaseya worked in earnest for three months to resolve flaws in its VSA monitoring and management software but ultimately lost the race with ransomware attackers, Dutch researchers say.

On Wednesday, the researchers who had found flaws in VSA released a timeline and description of issues that give more context to the engineering challenges Kaseya faced.

https://www.bankinfosecurity.com/kaseya-raced-to-patch-before-ransomware-disaster-a-17006

Click above link to read more.

Back to top

Workers careless in sharing and reusing corporate secrets

Businesses lose millions of dollars each year due to leaked enterprise infrastructure secrets including code, credentials, and keys, a new survey from 1Password found.

The report, which polled 500 IT and DevOps workers in the US in April, examines how organizations manage these types of sensitive information and corporate "secrets". Researchers found 65% of IT and DevOps employees estimate their company has more than 500 secrets and workers spend an average of 25 minutes each day managing this private information, at an estimated payroll expense of $8.5 billion annually across US companies. That amount has risen: 51% of respondents say their time spent managing secrets has increased in the last year.

https://www.darkreading.com/risk/workers-careless-in-sharing-and-reusing-corporate-secrets/d/d-id/1341480

Click above link to read more.

Back to top

Interpol arrests Moroccan hacker targets victims worldwide for stealing financial data

An alleged prolific cybercriminal has been apprehended in Morocco following a joint two-year investigation by INTERPOL, the Moroccan police, and Group-IB.

The alleged perpetrator, a citizen of Morocco, was arrested in May by the Moroccan police based on the data about his cybercrimes that was provided by Group-IB.

https://cybersecuritynews.com/interpol-arrests-moroccan-hacker/

Click above link to read more.

Back to top

Experts uncover malware attacks targeting corporate networks in Latin America

Cybersecurity researchers on Thursday took the wraps off a new, ongoing espionage campaign targeting corporate networks in Spanish-speaking countries, specifically Venezuela, to spy on its victims.

Dubbed "Bandidos" by ESET owing to the use of an upgraded variant of Bandook malware, the primary targets of the threat actor are corporate networks in the South American country spanning across manufacturing, construction, healthcare, software services, and retail sectors.

https://thehackernews.com/2021/07/experts-uncover-malware-attacks.html

Click above link to read more.

Back to top

Magecart hackers hide stolen credit card data info into images for evasive exfiltration

Cybercrime actors part of the Magecart group have latched on to a new technique of obfuscating the malware code within comment blocks and encoding stolen credit card data into images and other files hosted on the server, once again demonstrating how the attackers are continuously improving their infection chains to escape detection.

"One tactic that some Magecart actors employ is the dumping of swiped credit card details into image files on the server [to] avoid raising suspicion," Sucuri Security Analyst, Ben Martin, said in a write-up. "These can later be downloaded using a simple GET request at a later date."

https://thehackernews.com/2021/07/magecart-hackers-hide-stolen-credit.html

Click above link to read more.

Back to top

Trickbot malware returns with a new VNC module to spy on its victims

Cybersecurity researchers have opened the lid on the continued resurgence of the insidious Trickbot malware, making it clear that the Russia-based transnational cybercrime group is working behind the scenes to revamp its attack infrastructure in response to recent counter efforts from law enforcement.

"The new capabilities discovered are used to monitor and gather intelligence on victims, using a custom communication protocol to hide data transmissions between [command-and-control] servers and victims — making attacks difficult to spot," Bitdefender said in a technical write-up published Monday, suggesting an increase in sophistication of the group's tactics.

https://thehackernews.com/2021/07/trickbot-malware-returns-with-new-vnc.html

Click above link to read more.

Back to top