November 2024

Hacker Daily News

ISSA Information Systems Security Association Barbados Chapter

A review of the past month's vulnerabilities, hacks, cracks and cyber attacks.

The Securities and Exchange Commission (SEC) are still sifting through the details of the **2020 SolarWinds breach**. The SEC announced it has charged **four companies** for what the agency determined was an **intentional effort to minimize the impact of the hack to their systems**. Including: Unisys, Avaya Holdings Corp, Check Point, and Mimecast.

Unisys was dealt the largest civil penalty — **$4 million** — for its disclosure practices, as well as for controls violations.

"The SEC's order against Unisys finds that the company described its risks from cybersecurity events as hypothetical despite knowing that it had experienced two SolarWinds-related intrusions involving exfiltration of gigabytes of data," the SEC announcement of the fines read. "The order also finds that these materially misleading disclosures resulted in part from Unisys' deficient disclosure controls."

Source: https://www.darkreading.com/cyberattacks-data-breaches/sec-fines-companies-millions-downplaying-solarwinds-breach

Schubert Jonckheer & Kolbe LLP is investigating a cyberattack and data breach potentially affecting the private information of up to **14 million** customers of **American Water Works Company, Inc**., a New Jersey-based water and wastewater utility company that operates in **14 states** and manages **500 water systems**.

On October 7, 2024, American Water announced in a **Form 8-K** filed with the Securities and Exchange Commission that it experienced a cybersecurity incident. **The company shut down its MyWater customer portal and is pausing billing until further notice**.

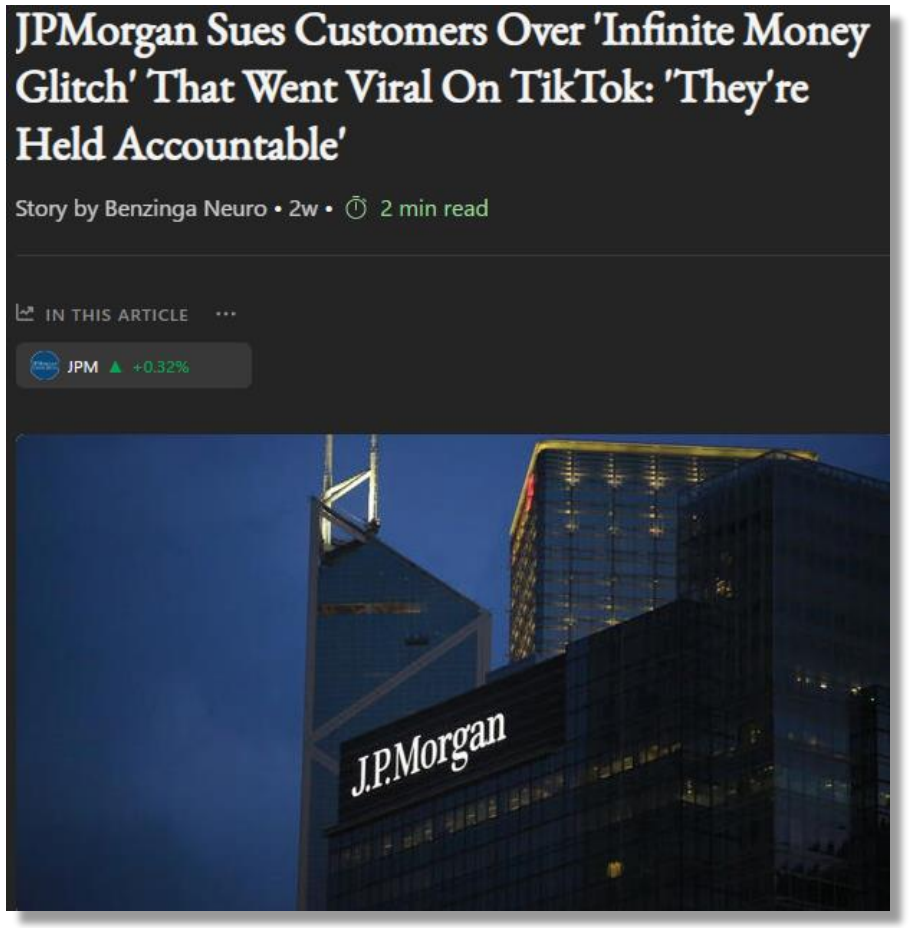
Source: https://www.darkreading.com/cyberattacks-data-breaches/american-water-under-investigation-for-cyberattack-potentially-affecting-14m-customers

An unknown threat actor has compromised Fortinet devices en masse across various industries, leaving no particular indication of what they plan to do next.

The campaign was enabled by a critical vulnerability, CVE-2024-47575, which the Cybersecurity and Infrastructure Security Agency (CISA) has just added to its Known Exploited Vulnerability (KEV) catalog.

According to Mandiant, a threat actor it now tracks as UNC5820 used CVE-2024-47575 to compromise more than **50 instances of FortiManager**. Doing so enabled them to siphon off information about the various devices connected to those FortiManager instances, which could prove useful in follow-on attacks. To this point, however, no malicious follow-on activity has been observed.

Source: https://www.darkreading.com/vulnerabilities-threats/critical-bug-exploited-fortinet-management-console

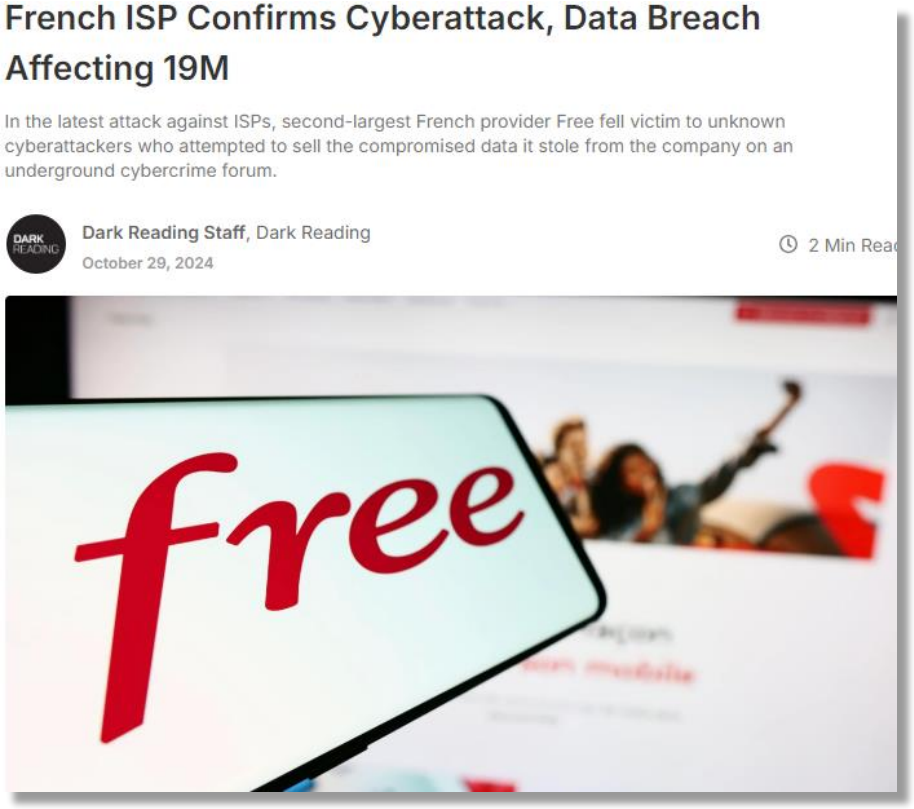


JPMorgan Chase & Co (NYSE:JPM) has initiated legal action against customers who allegedly **exploited a technical flaw to withdraw funds from ATMs before checks bounced**.

What Happened: The bank has filed lawsuits in three federal courts, targeting individuals who made the largest withdrawals during the '**infinite money glitch**' that gained attention on social media platforms like TikTok in late August, CNBC reported on Monday.

One such case in Houston involves **a man who owes JPMorgan $290,939.47 after an unidentified accomplice deposited a counterfeit $335,000 check at an ATM**. The bank alleges that the man began withdrawing the majority of the funds after the check was deposited.

Source: https://www.msn.com/en-us/money/news/jpmorgan-sues-customers-over-infinite-money-glitch-that-went-viral-on-tiktok-they-re-held-accountable/ar-AA1t6pHc



Free, a French telecommunications company and the second largest Internet service provider (ISP) in the country, has disclosed a cyberattack it fell a victim to over the weekend. It's the latest in **a line of attacks against ISPs and telcos of late**.

A threat actor stole information from the company's internal management tool, gathering data on the company's subscribers, and attempted to sell the data on the Dark Web in a cybercrime forum, the ISP confirmed to Agence France-Presse (AFP) on Oct. 26.

The hacker, known as "**drussellx**," posted a message on the forum, putting two databases stolen from the ISP company up for auction. The databases reportedly contained information on more than **19 million customer accounts**, and more than **5 million international bank account details**.

Source: https://www.darkreading.com/cyberattacks-data-breaches/french-isp-cyberattack-data-breach?s=03

The US Cybersecurity and Infrastructure Security Agency (CISA) has urged manufacturing companies to apply mitigations after one Rockwell Automation and several Mitsubishi systems were found to be vulnerable to cyber-attacks.

The vulnerabilities affecting Rockwell Automation FactoryTalk ThinManager, CVE-2024-10386 and CVE-2024-10387, are a missing authentication for critical function and an out-of-bounds read, respectively. Successful exploitation of these vulnerabilities could allow an attacker to send crafted messages to the device, resulting in database manipulation or a denial-of-service condition.

These critical vulnerabilities (CVSS scores of **9.3** and **8.7**) are exploitable remotely and require low attack complexity. Affected systems:

Rockwell Automation FactoryTalk ThinManager

Mitsubishi Electric FA Engineering Software Products

Mitsubishi Electric Multiple FA Engineering Software Products

Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series

Source: https://www.infosecurity-magazine.com/news/cisa-critical-vulnerabilities-ics/

An Android banking Trojan called **FakeCall** is capable of **hijacking the phone calls you make to your bank. Instead of reaching your bank, your call will be redirected to the cybercriminals.**

The Trojan accomplishes this **by installing itself as the default call handler on the infected device**. The default call handler app is responsible for managing incoming and outgoing calls, allowing users to answer or reject calls, as well as initiate calls.

Last time FakeCall reared its head, BleepingComputer reported that the malware was being distributed as fake banking apps that impersonate large financial institutions, as well as being distributed in phishing emails. When the receiver clicked a link in the email they'd download an Application Package (APK file) which acted as a dropper for the malicious app.

Source: https://www.malwarebytes.com/blog/news/2024/10/android-malware-fakecall-intercepts-your-calls-to-the-bank

An Iranian cyber-operations group, **Emennet Pasargad** — also known as **Cotton Sandstorm** — has broadened its attacks, expanding its targets beyond Israel and the United States and targeting new IT assets, such as IP cameras.

In an advisory published last week, the US departments of Justice and Treasury — along with the Israel National Cyber Directorate (INCD) — called out the change in tactics and noted that the group had provided resources and infrastructure services to Middle Eastern threat groups by operating as a legitimate company, Aria Sepehr Ayandehsazan (ASA).

In addition, since the beginning of the year, Emennet Pasargad has scanned for IP cameras, targeted organizations in France and Sweden, and actively probed a variety of election sites and systems, according to the government advisory.

Source: https://www.malwarebytes.com/blog/news/2024/10/android-malware-fakecall-intercepts-your-calls-to-the-bank

The City of Columbus, Ohio, has **notified 500,000 individuals that a ransomware attack in July 2024 stole their personal information**. In incident caused he city to take systems offline to contain the attack, impacting a range of services.

The city has since confirmed that allegedly stolen data has been placed on the dark web. This follows the city's attempt to sue researcher David Leroy Ross, also known as Connor Goodwolf, for informing local media of the theft of residents' personal data. Both sides have now reached an agreement to drop the case.

Source: https://www.securitymagazine.com/articles/101177-500-000-people-impacted-by-ransomware-attack-on-columbus-ohio

Trump attorney's phone tapped by Chinese hackers, sources tell CNN

By Paula Reid, Kaitlan Collins and Sean Lyngaas, CNN

2 minute read · Updated 9:42 AM EST, Fri November 8, 2024

The FBI has informed one of **President-elect Donald Trump's lead attorneys that his cellphone was tapped by Chinese hackers**, three sources familiar with the matter told CNN, as part of a wide-ranging operation targeting top Republicans and Democrats in US politics that has been underway for months.

The FBI informed the attorney, Todd Blanche, last week that the **hackers were able to obtain some voice recordings and text messages from his phone**, but that none of the information was related to Trump, one of the sources said. The FBI provided Blanche, who has had to start using a different number after the breach, what the hackers obtained, including communications with family, the source said.

Source: https://edition.cnn.com/2024/11/07/politics/trump-attorney-phone-tapped-chinese-hackers/index.html

The End

Prepared By:
Dwight Robinson
dwightrobinson.com