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

January 2022
Barbados has been reported to have its first ransomware attack of 2022. The Grief Ransomware Gang has the name of the local company disclosed as the victim of the attack and shows an invoice, payroll and employee badge IDs among the information exfiltrated during the attack.

Source: https://www.dbdigest.com/2022/01/ransomware-operator-claims-week-01-2022.html?m=1&s=03
With the preliminary voters list disclosed online ahead of the 2022 general election, there have been concerns raised by the public about the personal information being made available online.

The ISSA Barbados Chapter made a blog post advising the public about the risks associated with the disclosure and background information about the Representation of the People Act and amendments which lead up to the disclosure.
During the pandemic fake news about the virus, remedies and vaccines have perpetuated. Learn how to spot fake news effectively.

Checklist: How do I spot fake news?

- Fake news often appeals to emotions and instincts: Think about why the news appeals to you.
- Is it clear where the information came from? Check if it is from the original source. If it’s not, be skeptical.
- Does the person or website spreading the information seem credible? It’s worth taking a closer look.
- Sensational wording, a dubious layout or spelling mistakes should make you suspicious.
- Look for more information on the topic to compare and cross-check.
Computer maintenance workers at Kyoto University have announced that due to an apparent bug in software used to back up research data, researchers using the University's Hewlett-Packard Cray computing system, called Lustre, have lost approximately 77 terabytes of data.

Bermuda police say internet fraudsters have swindled the country's residents out of almost four million US dollars this year (2021).

The police said that “entire life savings” had been lost in some cases and authorities had managed to recover only US$40,600 of the haul.

Detective Chief Inspector, Sherwin Joseph, of the Bermuda Police Service's special investigations unit, said the cost of computer crime added up to more than US$3.8 million for the year.
Threat actors are actively **weaponizing** unpatched servers affected by the newly identified "**Log4Shell**" vulnerability in Log4j to install cryptocurrency miners, Cobalt Strike, and recruit the devices into a botnet, even as telemetry signs point to exploitation of the flaw nine days before it even came to light.

Source: https://thehackernews.com/2021/12/apache-log4j-vulnerability-log4shell.html?m=1
One of the largest Vietnamese crypto trading platforms, ONUS, recently suffered a cyber attack on its payment system running a vulnerable Log4j version.

Soon enough, threat actors approached ONUS to extort a $5 million sum and threatened to publish customer data should ONUS refuse to comply.

The crypto sector evolved massively from its initial form in 2009, but one major issue still persists when it comes to digital currencies – the risk of illicit entities, which would try to steal them.

And despite the technological advances of crypto projects in the past couple of years, in 2021 hackers got away with $4.25 billion worth of cryptocurrencies, which is almost a three-fold increase over 2020 and its $1.49 billion stolen in crypto assets.

A security researcher was able to change the results of an at-home COVID test and get those results certified by intercepting and modifying Bluetooth traffic from the device before it reached the app.

The process of falsifying results wasn’t a simple one — according to F-Secure’s writeup, the researcher used a rooted Android device to tap into and analyze the data the tester was sending to the app.

Source: https://www.theverge.com/2021/12/21/22847222/ellume-at-home-covid-test-bluetooth-android-certification
Microsoft's Digital Crimes Unit has disrupted the activities of a China-based hacking group called Nickel. Countries in which Nickel has been active include: United States, Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Panama, Peru, Trinidad and Tobago and Venezuela.

The attacks Microsoft's Threat Intelligence Center (MSTIC) observed are very sophisticated and use a variety of techniques, but they almost always had one goal: to insert hard-to-detect malware that facilitates intrusion, surveillance, and data theft. Sometimes, Nickel attacks used compromised third-party virtual private network (VPN) providers or stolen credentials obtained from spear phishing campaigns.

Source: https://www.guardian.co.tt/news/tt-among-several-countries-hit-by-cyberattacks-from-international-hacking-group--microsoft-6.2.1428159.21dafb6579
The carmaker, however, hasn’t provided any specifics on the hack itself, and while it did say an investigation is already underway, it wasn’t clear if its servers ended up infected with ransomware or not.

But as it turns out, this is exactly what happened, with ransomware group Snatch recently claiming the attack on its very own darknet website. The gang has also published screenshots with the stolen files, though no further specifics on the leak were shared.

TL; DR Breakdown

• Hackers drain $80 million from AscendEx
• Wallets on three blockchains were compromised including Ethereum, Polygon, and the Binance Smart Chain network
• Hackers are now targeting exchanges’ hot wallets

Crypto trading platform Bitmart said on it had experienced “a large-scale security breach” and that hackers had withdrawn about $150 million in assets. A third-party security firm, Peckshield, which first publicized the breach, put it closer to $200 million.

The affected ethereum and binance smart chain “hot wallets” carried only a “small percentage” of the exchange’s assets, according to the company.
Queensland’s CS Energy was the target of a sustained ransomware attack on Nov. 27, in what the utility’s chief executive officer has described as a worryingly accelerating trend.

The attack was thwarted before it had the potential to shut the company’s two thermal coal plants. Had the damage taken hold, it could have affected 35,000 megawatts of power, leaving 1.4 million to 3 million homes in the dark.
Microsoft has hit a new blow against a cyberespionage group coordinated from China. As the group has now announced, **42 domains were confiscated** that were used by the cyberespionage group **Nickel** alias **APT15**.

Microsoft had discovered some domains that were **used for data collection and transmission** to Nickel. A court in the US state of Virginia has now confirmed the confiscation of the domains.

For the last four years, a shadowy individual or organization known as ‘KAX17’ has been joining malicious servers to the Tor network, converting them into nodes at a time when the network is running out of bridges to evade censorship.

And, so far, all evidence point to KAX17’s objective to de-anonymize Tor users, according to cybersecurity experts.

That is, up to 10% of Tor nodes ended up in the hands of an unknown malicious actor; at the time, there was a 16% probability that a Tor user would connect to the network via one of KAX17’s servers... and a 35% likelihood that their traffic would be routed through one of its mid-nodes.
An internal guide to how the FBI can snoop on targets using data requested from nine companies and their services: Apple’s iMessage, Line, Signal, Telegram, Threema, Viber, Tencent’s WeChat, Meta’s WhatsApp and Wickr.

Information accessible include subscriber data, messenger sender-receiver data, device backup, IP address, encryption keys, date/time information, registration time information and user contacts. All but one (IP address) of iMessage can be accessed by the FBI.

The End