On December 28, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a vulnerability in KSMBD for Linux.
CIS Security Advisories

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN
30 December 2022

In The News This Week

The LastPass disclosure of leaked password vaults is being torn apart by security experts

Last week, just before Christmas, LastPass dropped a bombshell announcement: as the result of a breach in August, which lead to another breach in November, hackers had gotten their hands on users' password vaults. While the company insists that your login information is still secure, some cybersecurity experts are heavily criticizing its post, saying that it could make people feel more secure than they actually are and pointing out that this is just the latest in a series of incidents that make it hard to trust the password manager. LastPass' December 22nd statement was "full of omissions, half-truths and outright lies," reads a blog post from Wladimir Palant, a security researcher known for helping originally develop AdBlock Pro, among other things.... Read the rest of the article by Mitchell Clark here: The Verge

Contractor 'possibly' hacked and stole R77m from Postbank

Cape Town - The Postbank lost R77m in a 2021 hack of its IT systems and the breach was possibly committed by one of its contractors, Communications and Digital Technologies director-general Omega Shelembe has told MPs. - Three investigations were ordered into the hack, but the department has kept the details under wraps. Shelembe was responding to questions from DA MP Bridget Staff Masango on behalf of the department this week. The revelation comes a fortnight after the Cape Argus quoted Treasury Minister Enoch Godongwana as saying that the Federal Bureau of Investigation intercepted a hack attempt on the SA Reserve Bank in October this year. Masango had asked how much the Postbank had lost due to "hacking and theft" in the last three financial years. Shelembe did not offer much detail about the circumstances, except to divulge that the hack came at a cost of R77m to the department in the 2021/'22 financial year...
Read the full story by Soyiso Maliti here: The Cape Argus

Twitter in data-protection probe after '400 million' user details up for sale

A watchdog is to investigate Twitter after a hacker claimed to have private details linked to more than 400 million accounts. - The hacker, "Ryushi", is demanding $200,000 (£166,000) to hand over the data - reported to include that of some celebrities - and delete it. Ireland's Data Protection Commission (DPC) says it "will examine Twitter's compliance with data-protection law in relation to that security issue". Twitter has not commented on the claim. The data is said to include phone numbers and emails, including those belonging to celebrities and politicians, but the purported size of the haul is not confirmed. Only a small "sample" has so far been made public. The Guardian reported that data of US Congresswoman Alexandria Ocasio-Cortez was included in the sample of data published by the hacker. The data of broadcaster Piers Morgan, who recently had his Twitter account hacked, is also reported to be included. Twitter has so far not responded to press inquiries about the claimed breach..
Read the full article by Chris Vallance here: BBC News

Digital Assets of $9.9 Million Stolen in BitKeep Cyber Attack

Singapore-based decentralized multi-chain crypto wallet, BitKeep, confirmed on Wednesday that it was the target of a cyberattack that resulted in the theft of an estimated $9.9 million worth of digital assets. The attack, which took place on December 26, 2022, allowed threat actors to distribute fraudulent versions of BitKeep's Android app in an effort to steal users' digital currencies. The CEO of BitKeep, Kevin Como, has stated that the attack was a "large-scale hacking incident" in which malicious code was implanted into the Android app package (.APK) file uploaded on the BitKeep website. Due to the compromised APK, the hacker was able to steal users' private keys and transfer their cash. Moreover, BitKeep tweeted that the stolen funds were from BNB Chain, Ethereum, TRON, and Polygon. All monies were moved to just two addresses. However, over two hundred addresses on the other three chains were used in the attack. PeckShield, a blockchain security business, and OKLink, a multi-chain blockchain explorer, have both independently verified the incident and its estimated value in stolen funds. Users who have already downloaded the Android app's APK file for version 7.2.9 were not affected by the assault. Users who installed the software from a source other than Google Play, the App Store, or the Chrome Web Store were safe... Read the full article by Adeola Adegunwa here: InformationSecurityBuzz

Ransom Deadline Given By LockBit in Port of Lisbon Attack

The third largest port in Portugal has gone offline after the gang launched a ransomware attack on Christmas Day. Although this does not affect its operational activity, there has been nearly a week of extreme ambiguity, and LockBit claimed responsibility for the Port of Lisbon cyberattack. Visitors can still not access the main website, and no activity has been recorded since the attack. The Port of Lisbon, known as the pillar of the Portuguese economy for hundreds of years, brought commerce and employment to the people. The threat group has set January 18 as the deadline for payment and has stated that failure to do so could be detrimental to the Port of Lisbon. If the port fails to meet the demands of the Russian threat actor, the stolen data will be made public. Read the full story by Adeola Adegunwa here: InformationSecurityBuzz

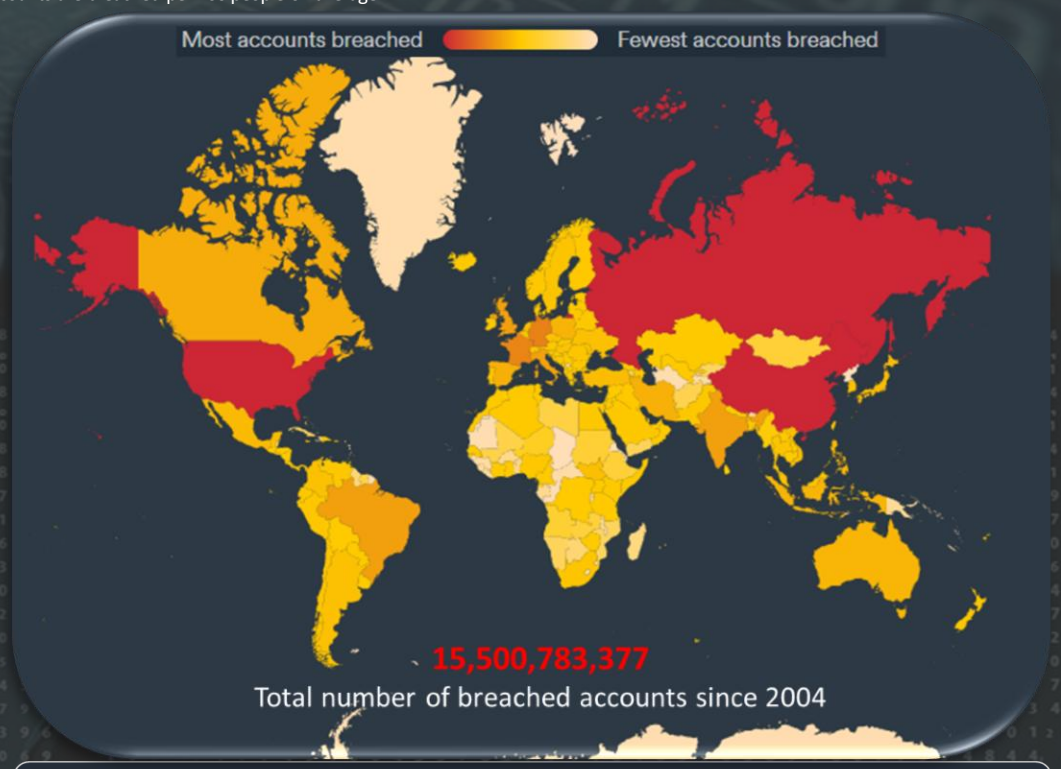
Surfshark Data Breach Report

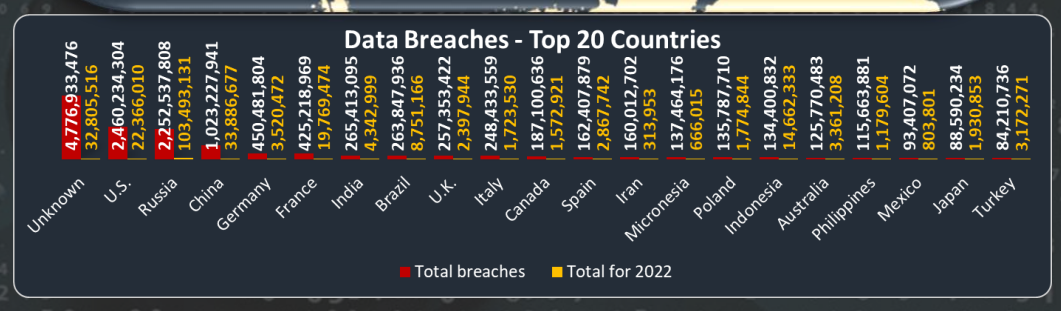
As we approach the end of the year, and as I reported on numerous data breaches this year, I was curious about the numbers in total. How many personal data breaches occurred globally, and how big is the problem really? Surfshark has been keeping stats on data breaches since 2004 and the numbers are staggering. Today, I want to share a glimpse into the global data breach problem and the numbers Surfshark has collected.

The below statistics shows publicly available information about personal data that's been copied, transmitted, viewed, and stolen from data holders, or otherwise illegally used since 2004.

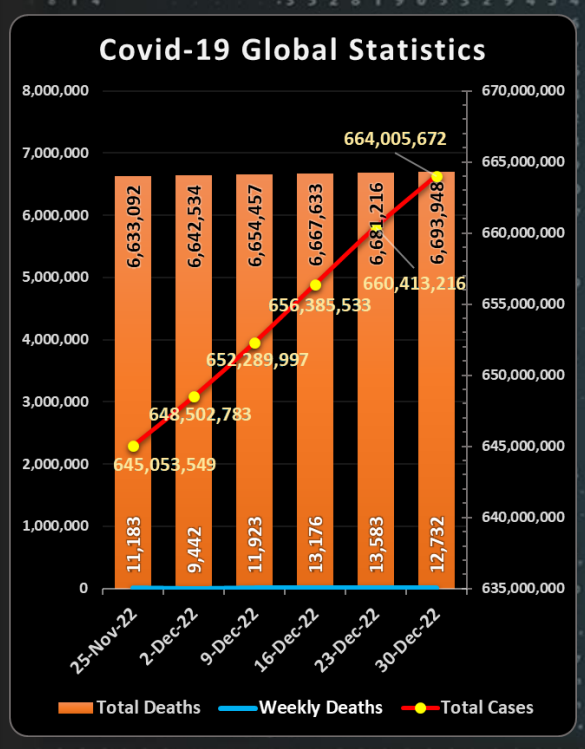
What you need to know about the numbers
This data is updated periodically, so make sure to check the numbers once in a while if you quote them. That said, there are two important things you should know about these numbers: (1) Most people use the same email for different accounts when registering online. That's why a single email or account can be breached several times in different cases and some numbers may seem so high (like 15.5B total breached accounts). (2) 30.8% of the total breached accounts did not contain information about a person's country of residence. So, the numbers of country-specific breaches are actually much higher than you see below.

Accounts get breached more than once
Since 2004, a total of 15.5B accounts have been breached and approximately 5.4B of them have unique email addresses. This means that on a global scale: (a) A single email address is breached 3 times on average. (b) 69 unique email addresses are breached per 100 people. (c) 199 accounts are breached per 100 people on average.





Visit Surfshark Data Breach Monitoring & Data breach monitoring full research material (updated monthly)

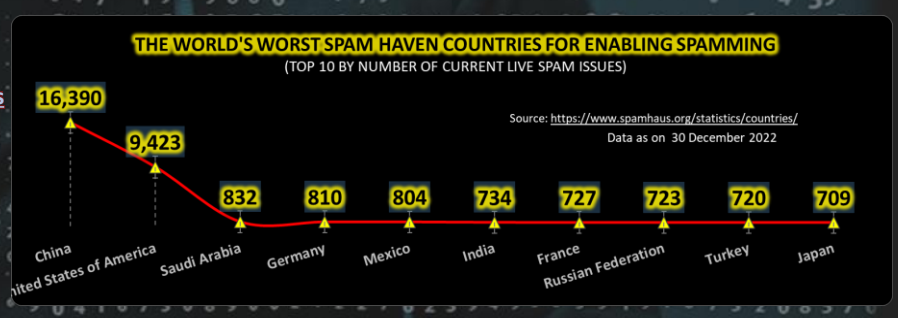


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- Will the Crypto Crash Impact Cybersecurity in 2023? Maybe.
- Stupid security 2022 – this year's infosec fails
- The Worst Hacks of 2022
- Cybersecurity in space: The out-of-this-world challenges ahead
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
Marine Traffic Track any Sailing Vessel globally
SatelliteXplorer Track satellites in orbit



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com