On December 7, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google products.
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
09 December 2022

In The News This Week

Apple announces new security and privacy measures amid surge in cyber-attacks

Encryption of iCloud storage means the information will be safeguarded from hackers as well as government agencies. - Apple announced a suite of security and privacy improvements on Wednesday that the company is pitching as a way to help people protect their data from hackers, including one that civil liberty and privacy advocates have long pushed for. The tech giant will soon allow users to choose to secure more of the data backed up to their iCloud using end-to-end encryption, which means no one but the user will be able to access that information. Apple says the changes will help users protect their digital lives from hackers in the exceptional case that an advanced state actor was able to breach the company servers. But privacy advocates like Albert Fox Cahn, founder of the Surveillance Technology Oversight Project, say these changes may have a more immediate effect on the types of user data law enforcement and government agencies can get from Apple.
Read the rest of the article here: The Guardian

Maryland is the latest state to ban TikTok in government agencies

ANNAPOLIS, Maryland — Maryland is banning the use of TikTok and certain China and Russia-based platforms in the state's executive branch of government, Gov. Larry Hogan said Tuesday, the latest state to address cybersecurity risks presented by the platforms. The Republican governor announced an emergency cybersecurity directive to prohibit the platforms' use, saying they could be involved in cyberespionage, government surveillance and inappropriate collection of sensitive personal information. "There may be no greater threat to our personal safety and our national security than the cyber vulnerabilities that support our daily lives," Hogan said in a statement, adding: "To further protect our systems, we are issuing this emergency directive against foreign actors and organizations that seek to weaken and divide us.“..
Read the full story here: NPR

Amnesty Canada target of China-linked cyberattack

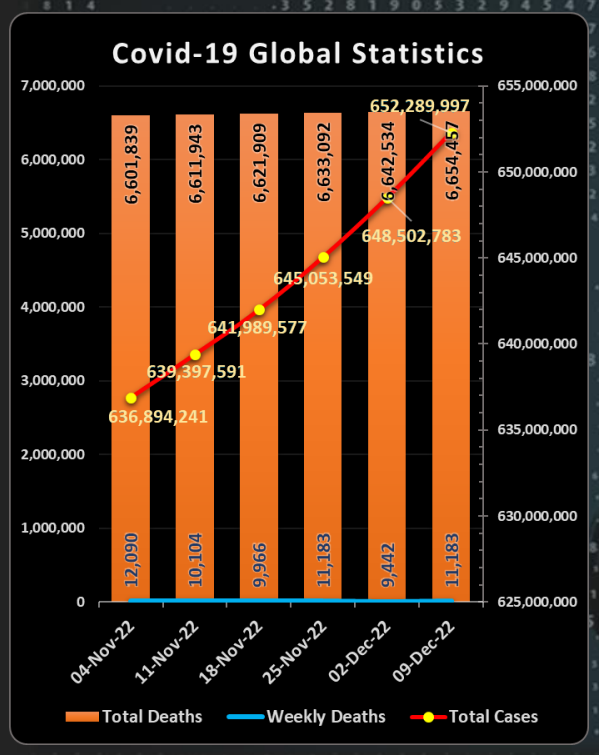
Rights group says it is publicising the attack to raise awareness of risks faced by civil society. - The Canadian office of human rights group Amnesty International says its English-language unit was the target of a “sophisticated” hacking attempt that it believes is linked to China. The digital security breach was first detected on October 5 when suspicious activity was spotted on Amnesty’s IT infrastructure, Amnesty International Canada said in a statement on Monday. It took immediate action to protect the systems and investigate the source of the attack, it added. “As an organization advocating for human rights globally, we are very aware that we may be the target of state-sponsored attempts to disrupt or surveil our work. These will not intimidate us and the security and privacy of our activists, staff, donors, and stakeholders remain our utmost priority,” Ketty Nivyabandi, secretary general of Amnesty International Canada, said in a statement.. Read the article here: Aljazeera

Cyberattack Shuts Down French Hospital

Patients transferred and operations cancelled following a recent network breach at a hospital in the outskirts of Paris. - French Health Ministry authorities were forced to shut down operations and transfer critically ill patients following a weekend cyberattack on a hospital outside Paris. Minister Francois Braun told France 24 that the hospital, which is located in Versailles, had been fending off regular ransomware attacks, along with many others in the area — including area hospital Corbeil-Essonnes, which was breached and unable to return to normal operations for weeks after refusing to pay a $10 million ransom. The region's health agency added that while hospital operations are halted, it is still doing everything possible to accept emergency walk-in patients until systems are recovered. Read the full story here: Dakreading

Russian Hackers Spotted Targeting U.S. Military Weapons and Hardware Supplier

A state-sponsored hacking group with links to Russia has been linked to attack infrastructure that spoofs the Microsoft login page of Global Ordnance, a legitimate U.S.-based military weapons and hardware supplier. Recorded Future attributed the new infrastructure to a threat activity group it tracks under the name TAG-53 and is broadly known by the cybersecurity community as Blue Callisto, Callisto, COLDRIVER, SEABORGIUM, and TA446. "Based on historical public reporting on overlapping TAG-53 campaigns, it is likely that this credential harvesting activity is enabled in part through phishing," Recorded Future's Insikt Group said in a report published this week. The cybersecurity firm said it discovered 38 domains, nine of which contained references to companies like UMO Poland, Sangrail LTD, DTGruelle, Blue Sky Network, the Commission for International Justice and Accountability (CIJA), and the Russian Ministry of Internal Affairs. It's suspected that the themed domains are likely an attempt on part of the adversary to masquerade as authentic parties in social engineering campaigns.
Read the rest of the article here: The Hacker News



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

Southern African power crisis

The power crisis in South Africa has escalated to stage 6 load shedding this week, and its neighbours are facing the same or even worse power problems. The problem is compounded with heightened cable theft made easier in areas where the power grid is switched off during load shedding. Cabe theft in South Africa is fuelled by the roaring illegal scrap metal trade.
As households and companies alike are experiencing power cuts for 8 hours or more a day, the question of business continuity and disaster recovery planning comes into play. What happens if the aging infrastructure collapse to a point where a total blackout is experienced for days or weeks on end, are businesses in South Africa prepared for this? Even for those who rely on generators, diesel fuel is in short supply and power generation in this way cannot be sustained for extended periods. And that also goes for our communication networks. Solar-powered cell towers are getting sabotaged, and batteries are stolen. For households, do they have alternative means for cooking and refrigeration?
What are the alternatives? Solar? Wind Power, Satellite Communication? Who knows what the future holds for the people in the Southern African region. Companies can plan and invest in renewable power sources, but not all households can afford the same.

How did it end up in this state of disrepair? I came across a few articles covering the issue this week and a Zimbabwean article (Bulawayo 24 News) by Eddie Cross sums it up for me. This and other extracts follows below.

Southern African power crisis stems from post-liberation history – By Eddie Cross

The electrical power crisis that has enveloped southern Africa has its roots in our post-liberation history. Prior to that, the utilities created by the States of southern Africa exhibited considerable foresight and planning. This was led by the power utility of South Africa which had visionary leadership at the time and like China in the past 50 years, turned their huge coal reserves into a cheap source of electrical energy. They installed enough power generation capacity to feed their own markets and to supply the deficit in their neighbours.

In Zimbabwe and Mozambique, their governments invested massively in the Kariba and Cahora Bassa dams with a combined capacity of 3 600 megawatts of cheap hydro electricity. The Kariba Dam remains the largest man-made dam in the world in terms of water storage capacity. These investments were well ahead of their time and contributed massively to regional power demand.

Southern Africa moved from the era of colonial and white domination to Independence and democracy and the new governments took for granted their self-sufficiency in power and did little to make the necessary investments to maintain self-sufficiency and to replace aging infrastructure. By the time they woke up to the fact, it was already too late to avoid a crisis in supply and distribution.

New power projects were planned - Medupi in the northern Limpopo River, Batoka in Zimbabwe and Zambia on the Zambezi River, but were bedevilled by corruption and poor project management. Zambia pulled the plug on Batoka and when the Medupi Power Station came on line - at three times the original cost, it failed massively and is still not producing. While this was happening, the older coal-fired power stations in the region were gradually coming to the end of their useful lives.

Then came the movement to restrict coal-fired power because of concerns about emissions. This was fully justified and I can remember driving through parts of the Transvaal and being shocked by the smell of the emissions from huge power plants and industrial installations like Sasol. In Zimbabwe, the power station built under sanctions during the Rhodesia era at Hwange Colliery with 900 megawatts capacity began to fail - old age and the mixed origin of second-hand components secured under UN sanctions. The older power plants in the main cities also served their time out and faced closure.

We were saved from a real crisis by two things, the collapse of the economy under the late former President Robert Mugabe which reduced power consumption and the decision to increase the power generation capacity at Kariba. The latter started in Zambia where they doubled the generation capacity on the northern bank and we followed with a similar expansion on the southern bank. Zambia went ahead with two dams and power plants on the Kafue River as well as a new "clean" coal-fired plant at Mamba coalfield in the south of the country.

But demand has continued to grow in the region - by about 5 000 megawatts a year. At the same time, power production started to decline and today the region is probably short of 15 000 to 20 000 megawatts of energy on a daily basis. This is not for want of trying and in both 2020 and 2021, new power generation capacity for roughly 5 000 megawatts a year came on stream throughout the region covered by the Southern African Power Pool. Even so, overall, the power generation situation deteriorated.

The main problem is South Africa but the situation on the Zambezi has also given rise to concern. When the Kariba Dam was designed it was on the basis that 100 years of rainfall records showed that the sustainable power generation capacity of the dam was about 1 100 megawatts on both sides of the wall. With the expansion of generation capacity to 2 200 megawatts, the yield of the dam has been doubled. That is what we see today - the water available for power generation has been exhausted and we are being forced to reduce generation to river flow levels.....

An article in AllAfrica stated the following: - **South Africans in The Dark About Severity of Electricity Crisis**
Power utility Eskom has been at the centre of South Africa's energy woes for more than a decade. The entity has been plagued by mismanagement, the breakdown of infrastructure at power stations, sabotage and corruption. The country's erratic electricity supply impacted businesses, with some saying it has led to wide-scale job losses.

South Africa's load shedding crisis has escalated again this week with the country facing a Stage 6 crisis - where 6,000 megawatts of power is shed. This would mean that businesses and households can be impacted up to 18 times for four days, at four-and-a-half hours at a time.
South Africans have been bombarded with continuing doom and gloom reports from Eskom. The most recent of which is that the utility is in desperate need of diesel to run the its coal-fired power stations. Diesel has been in short supply in the country, due to a lack of funding. In the meantime, citizens are forced to pay more for electricity - a service they are seeing very little of.

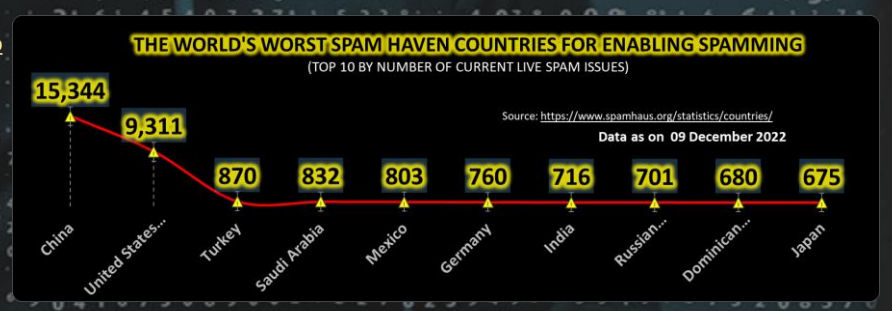
Finding sustainable forms of energy has been met with resistance - even at the highest level of government - when discussions around coal and its unsustainability as a resource was discussed by environmental groups. ..... The appointment of a new Eskom board has still not seen any change, as the country struggles on....

More on the subject can be found here: Financial Times, TechCentral

Other Interesting News and Cyber Security bits:

- 50 years since the last Apollo astronauts went to the moon, NASA is finally going back
- Drone-based security patrols: Mitigate the "human factor"
- US Army awards Kodiak Robotics $50 million contract for autonomous trucks
- 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