On February 3, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in GnuPG, Google and Apple products.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
05-Feb	105,393,496	2,292,533

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

05 February 2021

In The News This Week

Constitutional Court bans bulk Internet surveillance in South Africa

In a landmark judgment handed down on Thursday, the constitutional court banned the South African state from bulk surveillance of online communication, preventing security agencies from hoovering up Internet data. This sort of surveillance, which is routinely done by agencies such as the National Security Agency in the US and GCHQ in the UK – both of which have routinely tapped into submarine Internet cables – is now illegal in South Africa thanks to the country's highest court. The minister of state security had appealed an earlier high court judgment on the legality of bulk communication surveillance. The lower court had already declared bulk surveillance unlawful. The judgment by the constitutional court means the state has run out of legal options and any bulk surveillance is now unlawful and invalid. Read the full story by Duncan McLeod here: TechCentral

New Malware Hijacks Kubernetes Clusters to Mine Monero

Researchers warn that the Hildegard malware is part of 'one of the most complicated attacks targeting Kubernetes.' Researchers have discovered never-before-seen malware, dubbed Hildegard, that is being used by the TeamTNT threat group to target Kubernetes clusters. While Hildegard, initially detected in January 2021, is being used to launch cryptojacking operations, researchers believe that the campaign may still be in the reconnaissance and weaponization stage. Eventually, they warn, TeamTNT may launch a more large-scale cryptojacking attack via Kubernetes environments or steal data from applications running in Kubernetes clusters. Read the full story by Lindsey O'Donnell here: ThreatPost

Over a Dozen Chrome Extensions Caught Hijacking Google Search Results for Millions

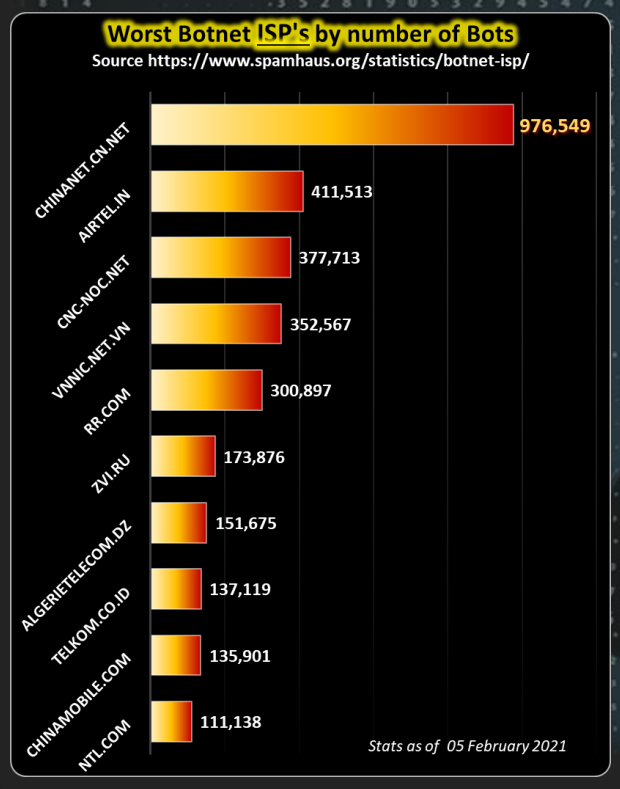
New details have emerged about a vast network of rogue extensions for Chrome and Edge browsers that were found to hijack clicks to links in search results pages to arbitrary URLs, including phishing sites and ads. Collectively called "CacheFlow" by Avast, the 28 extensions in question — including Video Downloader for Facebook, Vimeo Video Downloader, Instagram Story Downloader, VK Unblock — made use of a sneaky trick to mask its true purpose: Leverage Cache-Control HTTP header as a covert channel to retrieve commands from an attacker-controlled server. All the backdoored browser add-ons have been taken down by Google and Microsoft as of December 18, 2020, to prevent more users from downloading them from the official stores.
Read the full story by Ravie Lakshmanan here: TheHackerNews

Largest compilation of emails and passwords leaked for free on public forum

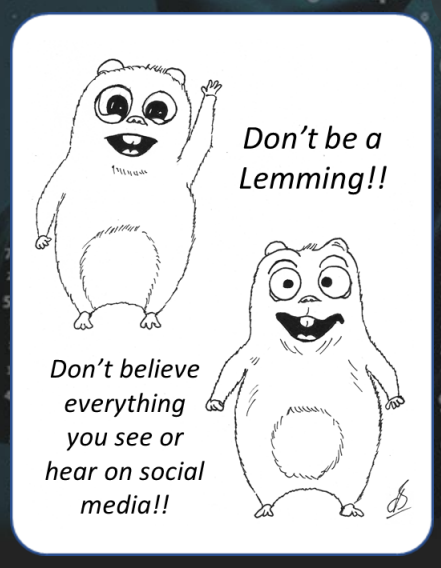
More than **3.2 billion** unique pairs of cleartext emails and passwords have just been leaked on a popular hacking forum, aggregating past leaks from Netflix, LinkedIn, Exploit.in, Bitcoin and more. This leak is comparable to the Breach Compilation of 2017, in which 1.4 billion credentials were leaked. However, the current breach, known as "Compilation of Many Breaches" (COMB), contains more than double the unique email and password pairs. The data is currently archived and put in an encrypted, password-protected container. The leaked database includes a script named count_total.sh, which was also included in 2017's Breach Compilation. This breach also includes two other scripts: query.sh, for querying emails, and sorter.sh for sorting the data. After running the count_total.sh script, which is a simple bash script to count the total lines in each of the files and add them together, we can see there are more than 3.27 billion email and password pairs. Read the full story by Bernard Meyer here: cybernews

239.4 million attempted attacks targeting healthcare alone in 2020

VMware Carbon Black released 2020 data that paints a holistic view of the threats healthcare organizations face and should be prepared for in 2021. Researchers found that there were 239.4 million attempted attacks targeting healthcare alone in 2020. VMware Carbon Black was also able to identify the top five ransomware families plaguing the healthcare industry including the following malware and ransomware strains: Cerber: 58%, Sodinokibi: 16%, VBCrypt: 14%, Cryxos: 8%, VBKrypt: 4%. "Amid the pandemic, cybercriminals now have limitless attack methods," said Rick McElroy, Principal Cybersecurity Strategist at VMware Carbon Black. "Whether it's using tried and true malware like EMOTET or using BitLocker to ransom systems, malicious actors continue to gain ground. Read the full story here: Security Magazine



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



TOP FAKE NEWS STORIES

A collection of wildly popular but untrue stories and news articles that floated around on social media in recent times.

5G Causes Covid-19

CLAIM: Covid-19 was caused by 5G radiation. (5G masts were attacked and set alight across Europe)
THE FACTS: Scientists confirm that COVID-19 is transmitted via respiratory droplets, and they are quick to point out that you cannot transmit droplets through 5G waves. Perhaps the most prevalent of all the theories is the suggestion that 5G degrades the immune system, and that this has helped spread COVID-19. Firstly, many of the hardest-hit countries currently have no 5G infrastructure. Iran has over 114,000 confirmed cases - and no 5G masts. Secondly, the theory that 5G is dangerous to the immune system is exactly the same claim we saw when 2G, 3G, 4G and Wi-Fi were all launched. 5G is in a band of low-frequency waves, like Wi-Fi, that are "non-ionising". The overwhelming weight of scientific evidence has shown that non-ionising radiation does not cause internal damage to our cells. So if we listen to the science, the simple fact is that 5G cannot be behind the pandemic, either by spreading the virus or by degrading our immune response. Source: Euronews

Dolphins in Venice

CLAIM: When Coronavirus lockdowns began, social media was abuzz with animal news. Nature was healing. Venice, no longer clogged with tourists, now had clean canals down which Dolphins cruised.
THE FACTS: Sadly, the heartening video was actually from a different region of Italy. The "Venetian" dolphins were filmed at a port in Sardinia, in the Mediterranean Sea, hundreds of miles away. Source: National Geographic

Trump commented on Amy Coney Barrett's appearance

CLAIM: When reporters asked President Donald Trump why he nominated Judge Amy Coney Barrett to replace the late Supreme Court Justice Ruth Bader Ginsburg, he said Barrett is "much better looking" than other women who have appeared on the court and "if people are more attractive, they get a fantastic amount of respect."
THE FACTS: There is no evidence Trump made these comments. His public remarks about Barrett since her nomination have centered on her qualifications for the court. Source: WJLA

Biden's tax plan spread online

CLAIM: Democratic presidential candidate Joe Biden's plan for capital gains tax means if you sell your home you will be taxed 40% of the profit.
THE FACTS: Social media users have been sharing misinformation about Biden's tax policy. The latest false claim states: "Biden's capital gains tax means that when you sell your home, you'll owe taxes of 40% of your profit! Let that sink in!" Tax experts familiar with Biden's tax proposal say the post is inaccurate for two reasons. For one, Biden's proposal to raise the maximum capital gains tax rate to 39.6% would only apply to people with incomes of over $1 million a year. Source: WJLA

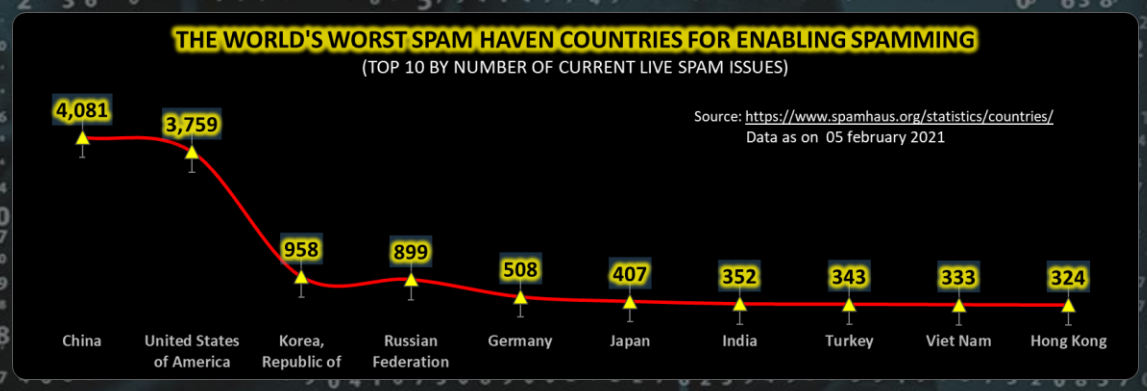
Trained Triceratops

CLAIM: In December 2020, a video went viral on social media of a purportedly real life and trained Triceratops being offloaded from a truck and mishandled by its handlers in Indonesia. Jurassic Park came to town? The video comes with the caption "Alhamdulillah piaraan baru udah nyampe", which translates to "Praise God, the new pet has arrived". It had over a million views within a week. One tweet even read "These are the signs of the end of time. Many strange animals have appeared"
THE FACTS: While the Triceratops looks unnervingly realistic, it is actually a very elaborate costume that was done up for Mojosemi Forest Park's promotional holiday video, and hidden underneath the dinosaur were a bunch of park employees, Indonesian media reported. Mojosemi Forest Park is in Indonesia's East Java province. The park has a special exhibit dedicated to our extinct buddies. Source: AsiaOne

Tokyo Olympics to be cancelled

CLAIM: The Times posted an article in January, siting an unidentified senior member of Japan's ruling coalition, as saying the games are doomed and will be cancelled.
THE FACTS: TOKYO (Reuters) - Japan and the IOC stood firm on Friday on their commitment to host the Tokyo Olympics this year and denied a report of a possible cancellation, although the pledge looks unlikely to ease public concern about holding the event during a pandemic. A government spokesman said there was "no truth" to a report in Britain's Times newspaper that the government had privately concluded the Games would have to be cancelled. Source: Reuters

These represent just a small sample of the myriad of fake news and tales that are spread on a daily basis by many different actors. Motives vary from political, environmental, sensational, criminal and some just for kicks. Don't be duped in believing everything that comes your way in social media. Fake news is aimed to invoke an emotional response that can lead to action that favours the perpetrators. Do some homework before sending it on, if you are not sure, ask a security professional to check it out for you, or simply ignore it and carry on with your life.



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