On December 22, the Cyber Threat Alert Level was evaluated and is being lowered to Blue (Guarded) due to vulnerabilities in Apache products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
24 Dec	278,580,422	5,402,483

Deaths this week: 48,819

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
24 December 2021

In The News This Week

4-Year-Old Microsoft Azure Zero-Day Exposes Web App Source Code

The Microsoft Azure App Service has a four-year-old vulnerability that could reveal the source code of web apps written in PHP, Python, Ruby or Node, researchers said, that were deployed using Local Git. The bug has almost certainly been exploited in the wild as a zero-day, according to an analysis from Wiz. The firm dubbed the vulnerability "NotLegit," and said it has existed since September 2017. The Azure App Service (aka Azure Web Apps) is a cloud computing-based platform for hosting websites and web applications. Local Git meanwhile allows developers to initiate a local Git repository within the Azure App Service container in order to deploy code straight to the server. After deployment, the application is accessible for anyone on the internet under the *.azurewebsites.net domain... Read the rest of the story by Tara Seals here: ThreatPost

CISA releases Apache Log4j scanner to find vulnerable apps

The Cybersecurity and Infrastructure Security Agency (CISA) has announced the release of a scanner for identifying web services impacted by two Apache Log4j remote code execution vulnerabilities, tracked as CVE-2021-44228 and CVE-2021-45046. "log4j-scanner is a project derived from other members of the open-source community by CISA's Rapid Action Force team to help organizations identify potentially vulnerable web services affected by the log4j vulnerabilities," the cybersecurity agency explains. This scanning solution builds upon similar tools, including an automated scanning framework for the CVE-2021-44228 bug (dubbed& Log4Shell)& developed by cybersecurity company FullHunt. The tool enables security teams to scan network hosts for Log4j RCE exposure and spot web application firewall (WAF) bypasses that can allow threat actors to gain code execution within the organization's environment. Read the rest of the story by Sergiu Gatlan here : Bleeping Computer

China suspends deal with Alibaba for not sharing Log4j 0-day first with the government

China's internet regulator, the Ministry of Industry and Information Technology (MIIT), has temporarily suspended a partnership with Alibaba Cloud, the cloud computing subsidiary of e-commerce giant Alibaba Group, for six months on account of the fact that it failed to promptly inform the government about a critical security vulnerability affecting the broadly used Log4j logging library. "Alibaba Cloud did not immediately report vulnerabilities in the popular, open-source logging framework Apache Log4j2 to China's telecommunications regulator," Reuters said. "In response, MIIT suspended a cooperative partnership with the cloud unit regarding cybersecurity threats and information-sharing platforms. Read more here: The Hacker News

Uber Ex-Security Chief Faces Additional Charges Of Wire Fraud

In addition to earlier accusations relating to concealing up a 2016 data breach that affected the personal information of 57 million drivers and users, Uber Technologies' former top security officer Joseph Sullivan now faces fresh wire fraud allegations. The Justice Department said in a statement that a superseding indictment handed down Wednesday reveals how Sullivan allegedly coordinated the payment of a six-figure sum to two hackers in exchange for their quiet about the breach. In a statement, Acting U.S. Attorney Stephanie M. Hinds stated, "We believe Sullivan forged records to evade the duty to notify victims and concealed the gravity of a severe data breach from the FTC, all to profit his corporation."... Read the rest here: TR Digital

Significant reform to Australia's cyber security laws with passage of critical infrastructure reforms

- Australia - Amendments to the Security of Critical Infrastructure Act 2018 (Cth) make company directors personally accountable for a cyber breach, requiring a highly proactive cyber security strategy. - Around the world, there has been an alarming rise in the number of threats against critical infrastructure. In response, the first part of the Government's planned changes to the Security Legislation Amendment (Critical Infrastructure) Bill 2021 have now been passed and came into effect on 2 December 2021 (the Act). The Act amends the previous Security of Critical Infrastructure Act 2018 (Cth) (previous Act), which governs domestic security risks of espionage, sabotage and coercion presented by foreign interference on our national critical infrastructure, and significantly increases the capacity of the Federal Government to enforce obligations for "critical infrastructure" assets... Read the rest of story by Clayton Utz here: Lexology

Cyber Attack - What if the Internet shuts down completely?

I was doing my usual browsing on security topics when I came about this article in the New Statesman publication, and it tickled my interest straight away as I thought, "what if the Internet really closes down or gets locked up?", that could be a disaster of epic proportions. Below I share an extract of the article which can be found on the New Statesman site.

Just as a viral pandemic was inevitable, a cyber pandemic in the future is also predictable. As technology is globally interconnected, a cyber virus could move from device to device, much like Covid-19 among humans. A virus propagated through an app could have devastating consequences, with the possibility of a global internet lockdown. The World Economic Forum has predicted that a **single day without the internet could cost more than $50bn globally**, even before considering the societal damage related to shutdown of essential services. Just as we must look to the future to prepare for the next pandemic, so too must we explore our global preparedness for cyber security threats.

At a recent round-table event hosted online by the New Statesman and sponsored by Fortinet and Hexaware, a group of policymakers and industry experts gathered to discuss cyber pandemic preparedness. They discussed future strategies, how best governments and businesses can promote cyber security, and how we can anticipate, and protect from, future attacks.

They agreed that when considering any strategy, the cyber hygiene practices of individuals needed careful consideration. Matt Warman MP, the former minister for digital infrastructure, drew attention to the consideration of who is behind cyber attacks – not just where the attacks are coming from, but why they are able to happen and where the weaknesses may stem from. "The vast majority of problems come not actually from incredibly sophisticated attackers, be they states or anyone else – they come from the carelessness of individual users who happen to have important jobs where they may or may not have a duty to know better," he said.

Chris Parker, director of government and defence at Fortinet, agreed, but also added that we should not disregard the seriousness of state-sponsored threats and the need for advanced detection and response systems in order to deal with "very, very aggressive attacks" at a "state-sponsored high level".

Gaurav Agrawal, vice president and infrastructure management services (IMS) practice head at Hexaware Technologies, warned of the "unknown track" and for any strategy to be prepared for "that absolute unforeseen situation". As such, strategy should prioritise pre-emption and prevention, as well as focusing on building resiliency and recovery programmes for when cyber attacks do succeed. Khalid Mahmood MP, member of the All-Party Parliamentary Group on Cyber Security, agreed with Agrawal that prevention is of the utmost importance, but also felt that any strategy should prioritise current vulnerabilities. He pointed to previous attacks on colleges and other vulnerabilities in the public sector, and that this needed to be addressed before we start to look at prevention.

When considering what businesses and governments can do to promote cyber security, Warman felt that there should be an awareness, but not a complacency, in the emergence of future technologies and the risks associated with them. For Warman, the emergence of future technologies drew up questions about the security of legacy systems in government and business. "It's partly how we address those legacy weaknesses, but it's also how do we try, in the future, to automate improvement?" he said.

Mahmood stated that though he was pleased to hear the UK government had pledged to invest £86m as part of funding for local governments and councils to ensure their cyber defences were robust, more needed to be done to educate the public and small business owners about the risk of cyber threats. "We really have got to have a national public campaign to make people aware of this," he said. "People are doing a fantastic job, but it's got to extend out to the wider community."

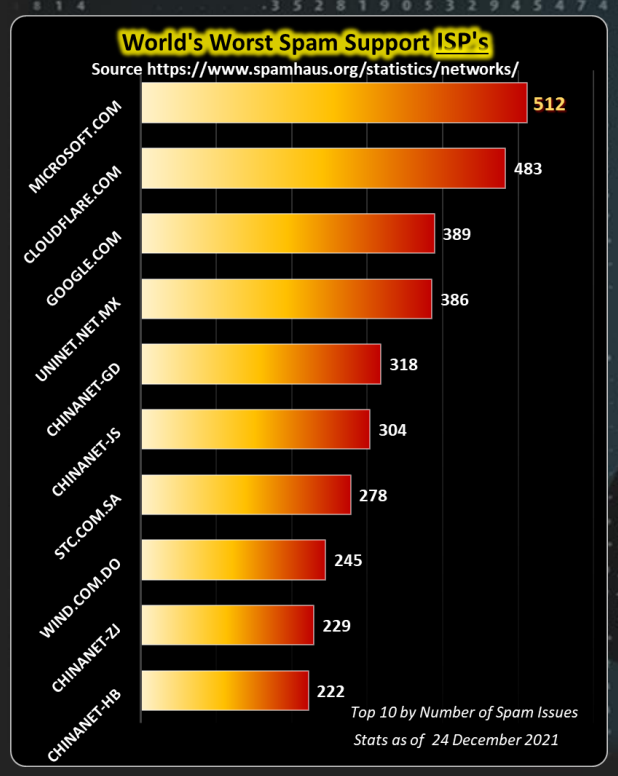
When it came to anticipating and reacting to future attacks, the attendees agreed that AI has a key role to play, acting as a kind of "arms race" against attackers. Parker talked about the uncertainty of future threats, and the prospect of a threat that no one has seen before: "You can build a very large fence that someone will build an even bigger ladder." However, he was positive about the capability of sophisticated AI technology to "patrol" security systems and keep future threats at bay: "Good technology, good systems proven around the world, are available, and they're not going to cost the earth for the taxpayer."

Mahmood compared the race to a never-ending game of chess, where one is trying to defend and the attacker is trying to overcome that defence. As such, Mahmood suggested that we protect our knowledge and consider licensing our learnings in order to restrict other actors from joining in. "You wouldn't be giving your codes to nuclear submarines to anybody else, so why are we doing this?" he asked.

Agrawal was also positive about the capabilities of technology to determine future threats; however, he pointed out that there are still major security and compliance concerns around these new technologies: "There are tools and technologies missing [protections around] enabling and applying security, compliance and guardrails across your private clouds, public clouds and data centres."

The round table concluded with a discussion of what IT managers and policymakers can do to ensure their systems are better protected. Agrawal suggested that identifying the motives of attacks right now was the best method of prevention, giving us an understanding of user behaviour and patterns. In terms of training employees, Parker suggested that companies make the most of the training provided by good cyber security suppliers, as well as the National Cyber Security Centre's training programmes. Warman also suggested that a kind of regulation of cyber security qualifications may provide people with a map for their future careers, in addition to softer forms of promotion and advertising of cyber skills by the government.

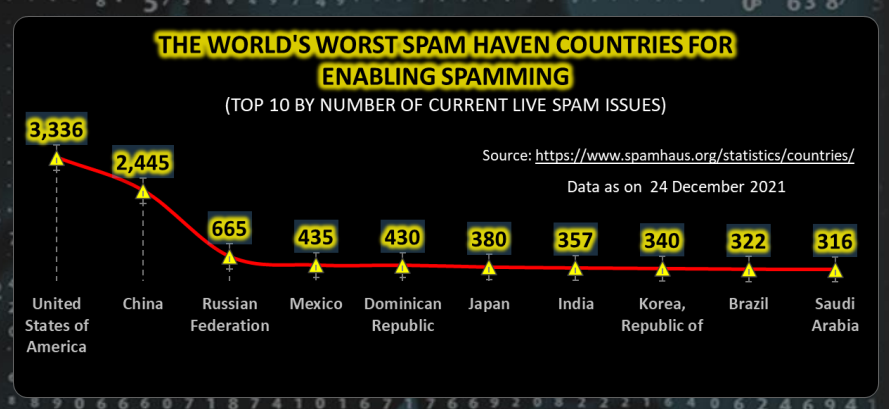
References: The New Statesman, World Economic Forum, Netblocks Calculator



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

Other Interesting News and Cyber Security bits:

- Total Cost Impact Calculator If the internet shuts down – By NetBlocks
- IoT SAFE — An Innovative Way to Secure IoT
- Nearly 50% of People Will Abandon Sites Prohibiting Password Reuse
- Five Nights at Freddy's: Security Breach Update 1.04 Patch Notes



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