On December 29, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to reported and observed exploitation of recently disclosed vulnerabilities, including log4J.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
31 Dec	286,942,665	5,447,836

Deaths this week: 45,353

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
31 December 2021

In The News This Week

T-Mobile says new data breach caused by SIM swap attacks

T-Mobile confirmed that recent reports of a new data breach are linked to notifications sent to a "very small number of customers" who fell victim to SIM swap attacks. - "We informed a very small number of customers that the SIM card assigned to a mobile number on their account may have been illegally reassigned or limited account information was viewed," a T-Mobile spokesperson told BleepingComputer. "Unauthorized SIM swaps are unfortunately a common industry-wide occurrence, however this issue was quickly corrected by our team, using our in-place safeguards, and we proactively took additional protective measures on their behalf. "T-Mobile refused to provide additional details when asked for more info on the total number of affected customers and the method used by the attackers to pull off the SIM swap attacks successfully. "We are not providing any additional information at this time. Thank you!," a company spokesperson told BleepingComputer.
Read the rest of the story by Sergiu Gatlan here: Bleeping Computer

Chinese APT Hackers Used Log4Shell Exploit to Target Academic Institution

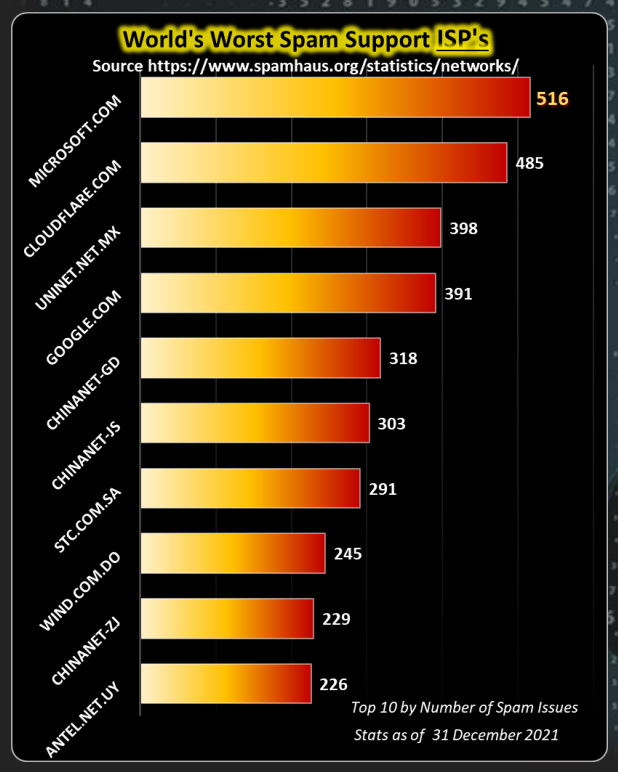
A never-before-seen China-based targeted intrusion adversary dubbed Aquatic Panda has been observed leveraging critical flaws in the Apache Log4j logging library as an access vector to perform various post-exploitation operations, including reconnaissance and credential harvesting on targeted systems. Cybersecurity firm CrowdStrike said the infiltration, which was ultimately foiled, was aimed at an unnamed "large academic institution." The state-sponsored group is believed to have been operating since mid-2020 in pursuit of intelligence collection and industrial espionage, with its attacks primarily directed against companies in the telecommunications, technology, and government sectors.
Read the rest of the story by Ravie Lakshmana here : The Hacker news

Volvo Security Breach Led to R&D Data Theft by 'Snatch' Threat Actors

Swedish automaker Volvo Cars confirmed a cyber security breach that allowed hackers to access its research and development data. - The company disclosed that a third party illegally accessed one of its file repositories, including limited R&D data during the intrusion. Volvo's investigation found that the incident could have effects on its operations. Subsequently, the Snatch cyber threat group added Volvo's logo and screenshots of allegedly stolen data to its data leak site and leaked 35.9 MB as proof of responsibility. Based in Gothenburg, Sweden, the Chinese Geely Holdings-owned manufacturer employs about 40,000 people globally. Its sales were over $15 billion in the first half of 2021, and the company had this year's largest IPO in Europe on October 29. Volvo's data breach notification said it acted "immediately and implemented security countermeasures including steps to prevent further access to its property and notified relevant authorities." The company also commenced an investigation into the security breach and involved a third-party cybersecurity specialist. Preliminary results of the probe confirmed that an unauthorized party illegally accessed the company's R&D data. Read more here: CPO Magazine

Ransomware gang coughs up decryptor after realizing they hit the police

The AvosLocker ransomware operation provided a free decryptor after learning they encrypted a US government agency. Last month, a US police department was breached by AvosLocker, who encrypted devices and stole data during the attack. However, according to a screenshot shared by security researcher pancak3, after learning that the victim was a government agency, they provided a decryptor for free. While they provided a decryptor to the police department, the ransomware operation refused to provide a list of stolen files or how they breached the department's network. A member of the AvosLocker operation told BleepingComputer today that they have no policy on who they target but usually avoid encrypting government entities and hospitals. "You should note, however, that sometimes an affiliate will lock a network without having us review it first," the AvosLocker operator told BleepingComputer. When asked if they purposely avoid targeting government agencies out of fear of law enforcement, they said it's more because "tax payer money's generally hard to get. "However, international law enforcement operations have resulted in numerous indictments or arrests of ransomware members and money launderers over the past year. These arrests include members of the REvil, Egregor, Netwalker, and Clop ransomware gangs. Read the rest of the article by Lawrence Abrams here: Bleeping Computer



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

CYBER SECURITY PREDICTIONS FOR 2022 AND BEYOND?

Last week Mandiant, a subsidiary of FireEye, released a report with cyber security predictions for 2022, which made for some interesting reading. There are 14 predictions in the report ranging from ransomware to IoT, and it deals with the stark reality of criminal advancement and persistent nation-state threats. This week I want to share a summary of some of the more significant predictions, but please visit the Mandiant site to read the full content of the report.

RANSOMWARE, MULTIFACETED EXTORTION, STATE SPONSORED ATTACKS AND OTHER PREDICTIONS

- No End in Sight: Increased Frequency and Expanding Tactics

The ransomware threat has grown significantly throughout the past decade and it will continue its upward trend. The business of ransomware is simply too lucrative, unless international governments and technology innovations can fundamentally alter the attacker cost-benefit calculation. While we have seen efforts to disrupt operations and hold threat actors accountable, cyber criminals simply sign up with another platform "as part of the ransomware-as-a-service business model" to continue their operations. We expect to see an increase in ransomware incidents against critical industries, where the urgency to pay is greater to avoid significant impact on the health and well-being of civilian populations. Threat actors engaged in multifaceted extortion will continue to find more ways to extort payments from their victims. Multifaceted extortion begins with locking victims out of their own files through encryption (classic ransomware), then adding threats such as making sensitive data public.

- No Honour Among Thieves: More Disputes Between Threat Actors

Ransomware-as-a-service operations regularly involve multiple actors, each one performing a specific element of the attack for a fee or a cut of the proceeds. We anticipate that there will be increased conflict amongst these actors throughout 2022, and that this conflict may ultimately lead to bad outcomes for victims. Conflicts may occur when targets don't pay, or if law enforcement disrupts threat actors' ability to get paid. Conflicts may also occur when victim organizations do end up paying; a specific actor may feel they didn't get paid enough or that they're not getting their fair share. In the next 12 months we expect to see many situations where victims will pay a million dollars or more to keep their stolen data from being published.

- Cyber Physical Systems Increasingly Under Threat from "n00bs"

Throughout 2021, we observed low sophistication threat actors learn that they could create big impacts in the operational technology (OT) space—perhaps even bigger than they intended. Actors will continue to explore the OT space in 2022 and increasingly use ransomware in their attacks. This targeting will occur because of the need to keep OT environments fully operational, especially when the systems are part of critical infrastructure. Attacks against critical OT environments can cause serious disruption and even threaten human lives

- OUTLOOK ON MAJOR NATION-STATE ACTORS: THE BIG FOUR

Major nation-state actors in Russia, Iran, China, and North Korea will likely maintain an aggressive posture to promote each of their regional interests. Russia's scope of operations will expand as it targets NATO, Eastern Europe, Afghanistan, and the energy sector. Iran will use its cyber tools to target Israel and the Middle East in an effort to shift power balances in its own interest. Using cyber espionage, China is poised to support the Belt and Road initiative and scale their operations. North Korea will flex its cyber capabilities and take risks despite its financial and geographical challenges

- DEEPFAKES: NOT JUST FOR INFORMATION OPERATIONS

The effectiveness of deepfakes in information operations has been discussed in the security community, but state sponsored and financially motivated actors have also demonstrated growing interest in this technology. Mandiant observed posts and advertisements about deepfake technology in underground Russian and English language criminal forums throughout 2020 and 2021. Users on these underground forums advertised customized deepfake videos and images, as well as training for users to create their own manipulated media. Deepfake audio has facilitated business email compromise (BEC) type fraud schemes.

- CYBER OUTSOURCING INCREASES VELOCITY AND IMPACT OF MALICIOUS OPERATIONS

Outsourcing in malicious operations via mechanisms such as ransomware affiliate programs, exploit vendors, commercial contractors, malware vendors and freelancers contributes to both the increasing frequency and complexity of cyber threat activity. We see no signs that this will slow down in 2022. Blurring distinctions between financially motivated and state-sponsored operations in terms of both tools and talent, maturing legitimate and illegitimate markets for third-party tools and services, and growing specialization and commodification of cyber threat skills; particularly in cyber crime communities; all contribute to making more sophisticated capabilities accessible to a wider pool of nation-state sponsors and criminal actors.

- CLOUD AND THIRD PARTIES INTRODUCE NEW CHOKEPOINTS

Organizations will continue to increasingly rely on cloud and cloud-hosted third-party providers for primary business tasks, putting more pressure on those third parties to maintain both availability and security. If either of those features are disrupted, organizations must be prepared to work around interruptions and diagnose, address, and recover from an incident when they may have not been the primary target and may not have access to the full picture of the attack lifecycle in internal logs.

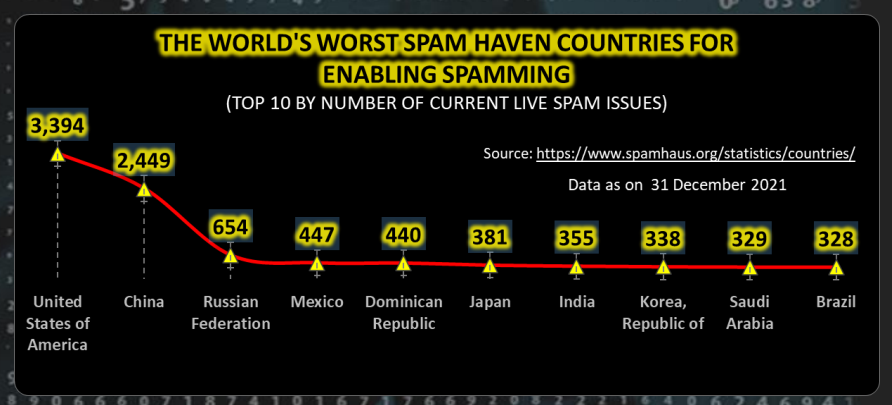
- MORE INTERNET OF THINGS DEVICES, MORE VULNERABILITIES, MORE ATTACK SURFACE

In the coming years, we expect to see a continued growth of Internet of Things (IoT) devices, many of which will be inexpensive and created without real consideration given to security. The number of vulnerabilities they introduce, in software and hardware, will make it hard for bug hunters to keep up. Because all these devices are connected, we'll see the general attack surface expand with the potential for serious impact. Unfortunately, there hasn't been enough emphasis on security in fundamental IoT device design to fix these issues, so the situation will only get worse in the years to come. When fixes are released for newly discovered vulnerabilities, the user must take the initiative to update their devices.

◊ **References:** Mandiant, MIT

Other Interesting News and Cyber Security bits:

- How Artificial Intelligence is changing cyber security landscape
- 4 Companies Control 67% of the World's Cloud Infrastructure
- United States Has the Most Data Breach Victims in the World
- Internet Safety 101 – Keep your kids safe from Cyber Bullying, Pornography, Traffickers, etc.



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