On December 15, the Cyber Threat Alert Level was evaluated and is being raised to Yellow (Elevated) due to vulnerabilities in Mozilla, SonicWall, Apache, Google, Apple, Microsoft, and Adobe products. CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
17 Dec	273,263,489	5,353,664

Deaths this week: 50,090

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
17 December 2021

In The News This Week

Log4j flaw: Thousands of attempts to exploit this severe vulnerability

Cyber attackers are making over a hundred attempts to exploit a critical security vulnerability in Java logging library Apache Log4j every minute, security researchers have warned. The Log4j flaw (also now known as "Log4Shell") is a zero-day vulnerability (CVE-2021-44228) that first came to light on December 9, with warnings that it can allow unauthenticated remote code execution and access to servers. Log4j is used in many forms of enterprise and open-source software, including cloud platforms, web applications and email services, meaning that there's a wide range of software that could be at risk from attempts to exploit the vulnerability. Meanwhile, cybersecurity researchers at Sophos have warned that they've detected hundreds of thousands of attempts to remotely execute code using the Log4j vulnerability in the days since it was publicly disclosed, along with scans searching for the vulnerability... Read the rest of the story by Danny Palmer here: ZDNet

Hackers Begin Exploiting Second Log4j Vulnerability as a Third Flaw Emerges

Web infrastructure company Cloudflare on Wednesday revealed that threat actors are actively attempting to exploit a second bug disclosed in the widely used Log4j logging utility, making it imperative that customers move quickly to install the latest version as a barrage of attacks continues to pummel unpatched systems with a variety of malware.. Read more here: TheHackerNews

West seeks to delay UN talks on cybersecurity — Russian presidential envoy

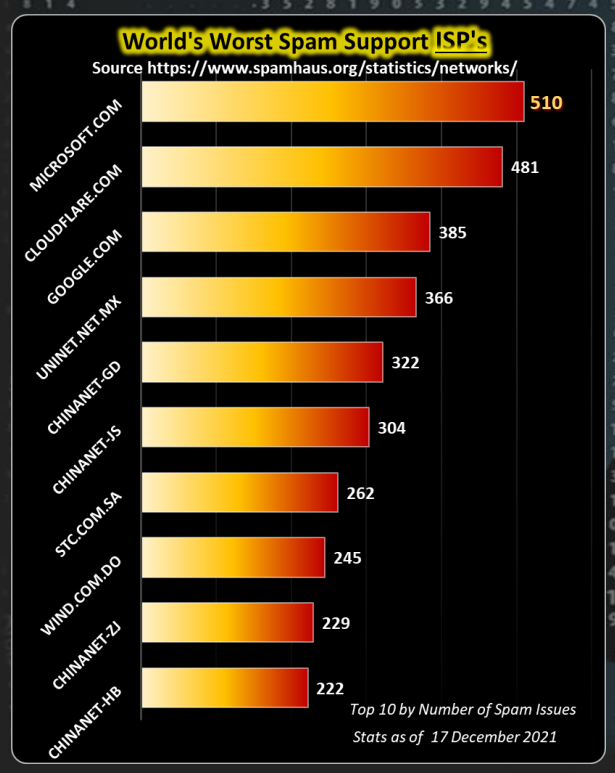
MOSCOW, December 16. /TASS/. A number of Western countries seek to delay cybersecurity negotiations on the United Nations platform, Russian Special Presidential Envoy for International Cybersecurity Cooperation Andrey Krutskikh said on Thursday at the Ninth All-Russia Congress of Political Scientists hosted by the Moscow State Institute of International Relations. "At this very moment, the United Nations is hosting the talks that Russia was promoting. It is a huge diplomatic achievement for us that we eventually came to an agreement and created a UN open-ended group to discuss cybersecurity issues," he pointed out. "Unfortunately, the talks have been stalled for three days because the Western countries - a group of 50 to 60 nations - who showed a different level of enthusiasm when voting against the launch of this negotiation process, are now replacing the issue of talks and a mandate agreed in June by asking who should engage in all these negotiations?"... Read more here: TASS News

60% of UK Workers Have Been Victim of a Cyber-Attack, Yet Awareness Remains Low

There is a "dangerous" lack of awareness among UK workers towards cybersecurity, leaving businesses at risk of attacks, according to a new study by Armis. This is despite 60% of workers admitting they have fallen victim to a cyber-attack. The nationwide survey of 2000 UK employees found that only around a quarter (27%) are aware of the associated cyber risks, while one in 10 (11%) don't worry about them at all. Even more worryingly, just one in five people said they paid for online security, putting businesses at high risk of attacks amid the shift to remote working during COVID-19. The most prevalent types of attacks experienced by workers or their organizations were phishing (27%), data breaches (23%) and malware (20%). The study also revealed growing concerns about the scale of the cyber-threats facing the UK. A large-scale cyber-attack was ranked as the fourth biggest future concern (21%) among the respondents, equal to the UK going to war. Two-fifths (40%) said they would like to see a minister for cybersecurity installed to ensure the issue is focused on more at a government level.... Read the rest of the article by James Coker here: Infosecurity Magazine

Kronos Ransomware Outage Drives Widespread Payroll Chaos

Kronos, the workforce management platform, has been hit with a ransomware attack that it says will leave its cloud-based services unavailable for several weeks – and it's suggesting that customers seek other ways to get payroll and other HR tasks accomplished. The outage has left cataclysmic issues for customers in its wake. Kronos offers a range of solutions for employee scheduling, compensation management, payroll and hours worked, benefits administration, time-off management, talent acquisition, onboarding, and more. It counts some of the largest companies in the world as its customers, such as Tesla and Puma, along with various health, public sector and university customers; organizations like the YMCA; and smaller businesses like restaurants and retailers... Read the rest of story by Tara Seals here: ThreatPost



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

Other Interesting News and Cyber Security bits:

- 'Cyber is the most dangerous weapon in the world,' JPMorgan council warns
- Gravitational Waves Should Permanently Distort Spacetime
- Top 20 Countries Found to Have the Most Cybercrime
- Russia poses the biggest nation-state cyber threat, says Microsoft

The year in review

As we get closer to the end of the year, we look back, and we can truly say, the cyber "war" has entered a new phase as governments realize both the dangers and potential of cyber security advances as a weapon. A nuclear warhead is a physical thing that we can deal with; the interconnected cyber world, on the other hand, is an ever-expanding intangible minefield. Apart from governments and their political agendas, cybercriminals are forever pottering around to find the next loophole or flaw to exploit this highly lucrative honeypot, as we've seen with the log4j flaw that wreaked havoc across the globe this week. We just don't know where the next attack is coming from, whether it is state-sponsored or criminally inspired. With that being said, I was looking around and found an article by John McClurg in the Security Magazine where he gives his take on the cybersecurity year in review. Please see an extract below.

John McClurg - 2021 passed as a whirlwind for those of us in cybersecurity. We experienced an accelerated shift toward a world in which its distinctions, definitions and categorical identities grew ever more porous.
The physical and digital worlds continued to merge, so much so that any barrier that had existed between them is now nearly gone. The growth of this porosity and its associated increase in attack vectors was exacerbated by expansion of the Internet of Things (IoT) and the more intertwined and connected environment it creates. This brings us to what we might consider the core of this year's challenges, as reflected in the SolarWinds and Colonial Pipeline compromises: the continued growth of successful ransomware attacks and the promulgation of the Executive Order regarding software bill of materials (SBOM). These events stand out as a reflection of what I consider most significant when it comes to what we saw in 2021 and are the basis of what we might expect to see in the year to come.

SolarWinds

Adding to the complexity evidenced in this compromise was the growth and acceptance of Continuous Introduction/Continuous Delivery (CI/CD) over the years as the backbone of modern-day DevOps operations. CI/CD represents an approach to software development that seeks to leverage shorter development cycles in delivering a steady stream of potentially disruptive innovations to customers who incessantly clamor for "more… faster." SolarWinds forced upon us an unsettling realization of the implications of a foundational system whose updates were compromised and propagated in the manner revealed. The contextual battlespace in which that propagation occurred was further exacerbated by the growing porosity mentioned above that makes up the modern supply chain, giving an adversary an almost unlimited number of "weakest leaks" through which to explore the options and realize the fruits of their efforts.

Colonial Pipeline

The lessons heralded by last May's Colonial Pipeline compromise were recently punctuated by the Iranian Gas Pumps affair. These taken-for-granted aspects of daily living don't have to be denied us for very long before an unacceptable pain settles in. The Colonial Pipeline, which supplies 45% of the East Coast's supply of various fuels, was taken offline after it was impacted by a ransomware attack. Now, on the other side of the world, another cyberattack has left drivers in Iran with virtually no fuel. The online attack reportedly crippled essentially every gas station across Iran — ironic, as that nation is a leading exporter of oil.

Ransomware on the Rise

The Colonial Pipeline affair was just one instance of how ransomware attacks took the headlines by storm in 2021 — notwithstanding the existence of validated, AI-supported math models whose prowess against such attacks continues to be well-documented. That an inertia seems to yet hold major Fortune 500 companies and infrastructures of nations prisoner and doggedly committed to outdated models of defense staggers rational comprehension. That modern ransomware attacks appear to easily circumvent the established pillars of traditional cyber protection punctuates the need to find new ways to solve this problem. Advancing the same old solutions while expecting different outcomes is the classic definition of "insanity."

Executive Order

Proving that the supply chain implications of these standout events did not go unappreciated, the U.S. presidential administration issued an Executive Order, the heart of which requires those who manufacture and distribute software a new awareness of their supply chain to detail what is actually in their products — particularly open-source software — and the ability to reflect that awareness in an accurate SBOM. With announced vulnerabilities growing ever more prevalent, these SBOMs will provide purchasers with a means of determining how relevant any announcement may be to their interests.

Where to Go From Here

Although predicting the future is a challenging business under the best of circumstances, it is perhaps made easier by the fact that we, as humans, so often refuse to learn from the past and are, therefore, condemned to repeat it, as George Santayana is often quoted as saying. Predicting the future thus becomes, in part, the practice of isolating those lessons we should have learned but did not and translating that into what we are then likely to experience again. Heraclitus of Ephesus opined that you can't step in the same river twice, but these repeat experiences should be similar enough to afford insights into what mitigating actions might be open to us. We've learned that, apparently, our math models can predict and continue to do so at least in the limited sphere of malware. They actually do know what attack will come next — oftentimes years in advance. In other spheres, we're not so fortunate. What we can do, however, is use the available information at hand to best prepare ourselves for every possible scenario. We know what technology is being developed and we know the potential risks that come with it. We've seen how adversaries can harness the power of good to do harm. It's up to everyone in the cybersecurity community to ensure smart, strong defenses are in place in the coming year to protect against those threats.

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