ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

May 11, 2022

FEDERAL AGENCIES LIKELY TO GET NEW CYBERSECURITY GUIDANCE 'IN COMING WEEKS'

Aaron Boyd | Nextgov | May 5, 2022

The Office of Management and Budget is preparing to release new requirements around software supply chain and cybersecurity, according to a top federal cybersecurity official. While discussing future priorities for federal cybersecurity during a Nextgov event Thursday, Steven Hernandez, chief information security officer for the Education Department and chair of the Federal CISO Council, said a new mandate on software supply chain is forthcoming. "I wouldn't be surprised if in the coming weeks we hear something from [the Office of Management and Budget] about what they want to do in the software space, in terms of the next step and building on what [the National Institute for Standards and Technology] put out," he said. Pushed to elaborate, Hernandez said policymakers have been working to codify efforts by NIST and other cybersecurity-focused pockets of government like the Cybersecurity and Infrastructure Security Agency, or CISA, to help agencies understand the provenance of software used on government networks and to hold vendors accountable for maintaining security over that code. "We're going to see a lot more discussion around software," Hernandez said.

Read the full article here.

PENTAGON FINDS HUNDREDS OF CYBER VULNERABILITIES AMONG CONTRACTORS

Colin Demarest | C4ISRNet | May 3, 2022

A U.S. Defense Department pilot program designed to root out digital vulnerabilities among contractors identified hundreds of flaws over the course of one year, organizers said. Cybersecurity researchers with bug bounty team HackerOne discovered some 400 issues across dozens of companies during the Defense Industrial Base-Vulnerability Disclosure Program, coordinated by the department's Cyber Crime Center and the Defense Counterintelligence and Security Agency. "[The program] has long since recognized the benefits of utilizing crowdsourced ethical hackers to add defense-in-depth protection to the DoD Information Networks," Melissa Vice, interim director of the vulnerability disclosure program, said in a statement. Vice added that the pilot was intended to identify whether similar critical and high-severity vulnerabilities existed for small-to-medium-cleared and non-cleared defense-industrial base companies with potential risks for critical infrastructure and the U.S. supply chain. Which contractors were involved was not disclosed. The campaign launched in April 2021 with 14 participating companies and 141 publicly accessible assets to examine.

Read the full article here.

CHINESE HACKERS TOOK TRILLIONS IN INTELLECTUAL PROPERTY FROM ABOUT 30 MULTINATIONAL COMPANIES

Nicole Sganga | CBS News | May 4, 2022

A yearslong malicious cyber operation spearheaded by the notorious Chinese state actor, APT 41, has siphoned off an estimated trillions in intellectual property theft from approximately 30 multinational companies within the manufacturing, energy and pharmaceutical sectors. A new report by Boston-based cybersecurity firm, Cybereason, has unearthed a malicious campaign — dubbed Operation CuckooBees — exfiltrating hundreds of gigabytes of intellectual property and sensitive data, including blueprints, diagrams, formulas, and manufacturing-related proprietary data from multiple intrusions, spanning technology and manufacturing companies in North America, Europe, and Asia. "We're talking about Blueprint diagrams of fighter jets, helicopters, and missiles," Cybereason CEO Lior Div told CBS News. In pharmaceuticals, "we saw them stealing IP of drugs around diabetes, obesity, depression." The campaign has not yet been stopped.

Read the full article here.

SOUTHERN ILLINOIS MATHEMATICS PROFESSOR CONVICTED OF HIDING CHINESE BANK ACCOUNTS

Christian Schneider | The College Fix | May 9, 2022

A federal jury has convicted a Southern Illinois University-Carbondale professor of failing to disclose a Chinese bank account on his tax returns between 2017 and 2019. Mingqing Xiao, a math professor at the university, could face up to five years in prison and a substantial fine after being found guilty on four counts of hiding his Chinese bank accounts. Xiao was indicted in April 2021 on two counts of wire fraud and one count of making a false statement. Last week District Judge Staci Yandle threw out the fraud charges and a jury acquitted Xiao of the false statement charge. Xiao's arrest was part of the U.S. Department of Justice's "China Initiative," a "broad, multi-faceted effort to counter Chinese national security threats and safeguard American intellectual property." The China Initiative was discontinued earlier this year amid charges it unfairly targeted professors of Chinese descent. The DOJ relabeled the program as a "strategy for countering nation-state threat" after deciding its previous name had had a "chilling effect on U.S.-based scientists of Chinese origin" and "fueled a narrative of intolerance and bias."

Read the full article here.

PENTAGON REPORT DETAILS 8 CASES REVEALING CHINA'S INFILTRATION INTO US COMPANIES

The BL Staff | The BL | May 9, 2022

A Department of Defense study has shown the Chinese government is making use of a U.S. government-program to serve their own interests. The Pentagon's Small Business Innovation Research program aims at promoting innovation among small U.S. companies. The awards process is competitive. However, according to the Wall Street Journal, the report finds that some program members have joined Chinese government talent programs. More importantly, they have continued to work at institutions that support China's People's Liberation Army. The report lists eight typical cases with quote "national and economic security implications" end-quote. One case was about a U.S. developer of polymer solar cells called Solarmer Energy Inc. Solarmer Energy Inc. received funding from the Pentagon and other agencies. However, the firm later dissolved its U.S.-based operation. Afterward, it moved its research, development, and intellectual property to a Beijing-based subsidiary. The subsidiary also works with a Chinese state-run lab and has conducted research with defense applications.

Read the full article here.

RESEARCHERS UNCOVER YEARS-LONG ESPIONAGE CAMPAIGN TARGETING DOZENS OF GLOBAL COMPANIES

Jonathan Greig | The Record by Recorded Future | May 5, 2022

Researchers with cybersecurity firm Cybereason briefed the FBI and Justice Department recently about Operation CuckooBees, an alleged espionage effort by Chinese state-sponsored hackers to steal proprietary information from dozens of global defense, energy, biotech, aerospace and pharmaceutical companies. The organizations affected were not named in Cybereason's report but allegedly include some of the largest companies in North America, Europe and Asia. Cybereason tied the campaign to the prolific Winnti Group, also known as APT 41. Cybereason CEO Lior Div told The Record that the most alarming aspect of the investigation into Operation CuckooBees was the evasive and sophisticated measures used to hide inside the networks of dozens of the largest global manufacturing companies in North America, Europe and Asia as far back as 2019. "The group operates like a guided missile and once it locks in on its target, it attacks and doesn't stop until it steals a company's crown jewels," Div said.

Read the full article here.

CANADIANS BEING TARGETED BY INTEL SERVICES LINKED TO CHINA, RUSSIA: REPORT

Anirudh Bhattacharyya | Hindustan Times | May 7, 2022

Canadian Security Intelligence Service (CSIS) noted "hostile intelligence services" linked to the governments of China and Russia continue to target Canadians for "intelligence collection and asset recruitment, according to a report released by the country's intelligence agency on Friday. In the Public Report 2021, tabled in parliament on Friday, the CSIS said that China, along with traditional spying activity, "relies on non-traditional collectors- individuals without formal intelligence training who have relevant subject matter expertise (i.e. scientists, business people), including those who are recruited via talent programs (i.e. scholarships, sponsored trips, visiting professorships, etc.) and other non-transparent means in Canada". It cited China's Thousand Talents Plan -- a programme started by the Chinese government in 2008 to bring back leading scientists and engineers from abroad -- as an example, adding that cyber actors linked to the Chinese state "continue to target multiple critical sectors within Canada".

Read the full article here.

SAFEGUARDING OUR FUTURE – PROTECTING PERSONAL HEALTH DATA FROM FOREIGN EXPLOITATION

The National Counterintelligence And Security Center | January 31, 2022

Foreign companies and some U.S. businesses with facilities abroad have been partnering or contracting with U.S. organizations to provide diagnostic tests and services that in some cases collect specimens, DNA, fitness / lifestyle information, or other personal health data from patients or consumers in the United States. Some of these companies may be subject to foreign laws that can compel them to share such data with foreign governments, including governments that exploit personal health data for their own ends and without regard to individual privacy. For example, several Chinese companies have partnered or contracted with U.S. organizations and are accredited, certified, or licensed to perform genetic testing or whole-genome sequencing on patients in the U.S. healthcare system, potentially giving them direct access to the genetic data of patients in the United States. Chinese companies are compelled to share data with the government of the People's Republic of China, which has used genetic data for state surveillance and repression of its ethnic and religious minorities, as well as for military research and applications.

Read the full article here.

OH GREAT, HACKERS FOUND A NEW WAY TO SNEAK MALWARE INTO YOUR COMPUTER

Jorge Jimenez | PC Gamer | May 9, 2022

Cybersecurity experts recently discovered a new technique for storing malware on an unsuspecting PC. Used by hackers, it involves slipping malware inside of Windows 11 event logs. To make matters worse, this new technique is designed to make the infection process nearly impossible to detect until it's too late. Researchers at Kaspersky (thanks Bleeping Computer) analyzed a recent sample of the malware on a customer's computer in February of this year. During their analysis, they found that a hacker was able to plant fileless malware into a victim's file system by hiding it away in your Windows events logs. A first, according to Kaspersky. This sophisticated attack injects shellcode payloads into Windows event logs into the KMS (Key Management Services) via a custom malware dropper and basically hides in plain sight. The dropper then loads malicious code by taking advantage of a DLL exploit and hides itself as a copy of a legitimate error file. So, even if you check your event logs, it'll look like nothing out of the ordinary. The attacker can then install a Trojan virus (or, in this case, a number of Trojans), which will wreak havoc on a system.

Read the full article here.

CHINA PLANS TO DUMP 50 MILLION FOREIGN PCS WITHIN THE NEXT TWO YEARS

Zach Marzouk | IT Pro | May 6, 2022

The Chinese government has reportedly ordered its central agencies and state-backed corporations to replace foreign-branded personal computers with domestic alternatives within the next two years. This is part of the country’s domestic plan to replace imported technology with local alternatives, as reported by Bloomberg. Staff have been asked to exchange foreign PCs for domestic alternatives that run on operating software developed in the country. The policy is estimated to eventually lead to the replacement of around 50 million PCs in the central government alone. The new initiative will involve dismantling the presence of HP and Dell Technologies, which are the country’s biggest PC brands after local provider Lenovo. PC shipments in China grew 9% in the last quarter of 2021 to reach 16.5 million units, according to Canalys. This finished a year of strong growth for the Chinese market, which saw shipments rise 10% in 2021 to a record 57 million units.

Read the full article here.

CYBER COMMAND CREATES FORUM WITH INDUSTRY TO SHARE THREAT INFORMATION

Mark Pomerleau | FedScoop | May 5, 2022

U.S. Cyber Command has created a collaborative program with the private sector to share insights and information about critical cyber threats in an effort to further bolster national cybersecurity. The program, dubbed “Under Advisement,” involves members of the command’s elite cyber national mission force (CNMF) — which is responsible for tracking and disrupting specific nation-state adversaries — sitting in chat rooms and disclosing threats with the cybersecurity sector, officials have said. These military personnel use their real names for the sake of transparency and actually talk to members of the private sector. “They are technical experts that can actually talk to people. They sit in private chats, elite invite-only industry forums, all in full name and with full transparent attribution,” Maj. Gen. William Hartman, commander of the cyber national mission force, said Wednesday during a speech at the Vanderbilt University Summit on Modern Conflict and Emerging Threats.

Read the full article here.

COMPETING FOR TALENT ON THE BATTLEFIELD OF THE GLOBAL SOUTH

Philip G Altbach and Hans de Wit | University World News | May 7, 2022

More than half a century ago, when universities around the world were beginning to focus on the various aspects of internationalisation, especially student mobility, most of those engaged in this nascent academic enterprise saw it as a way of providing students with an international experience and building global understanding. At about the same time, what we now term globalisation – increased interlinking of economies, more trade and the beginnings of the 'global knowledge economy' – was gaining steam. Higher education and research became core elements of all of these developments. In 1965, there were approximately 250,000 globally mobile students – a number that has grown to 5.6 million today. At the same time, broader aspects of globalisation were beginning to emerge, including labour mobility.

Read the full article here.

QUANTUM COMPUTERS ARE ALREADY DETANGLING NATURE'S MYSTERIES

Amit Katwala | WIRED | June 17, 2021

The lithium-ion battery is the unsung hero of the modern world. Since it was first commercialised in the early 1990s, it has transformed the technology industry with its ability to store huge amounts of energy in a relatively small amount of space. Without lithium, there would be no iPhone or Tesla – and your laptop would be a lot bigger and heavier. But the world is running out of this precious metal – and it could prove to be a huge bottleneck in the development of electric vehicles, and the energy storage solutions we'll need to switch to renewables. Some of the world's top scientists are engaged in a frantic race to find new battery technologies that can replace lithium-ion with something cleaner, cheaper and more plentiful. Quantum computers could be their secret weapon.

Read the full article here.

SAFEGUARDING OUR FUTURE – BEWARE OF FOREIGN GIFTS WITH STRINGS ATTACHED

The National Counterintelligence And Security Center | June 19, 2020

City-to-city partnership agreements could be used by foreign powers to advance a political goal or influence government decisions. What seems good for your city or state may undermine strategic U.S. interests. You may be manipulated to support a foreign malign narrative or hidden agenda. A foreign power may seek your support to gain a political or economic advantage. May receive sub-par donations while the donor receives a propaganda boon. Be aware of the consequences of your actions-locally and nationally. Understand your role and the potential press coverage your acceptance will draw. Beware of those who would ask you to advance a position or lobby on behalf of another nation or group. Beware of gifts of "smart" technology with potential for storing/transferring sensitive data.

Read the full article here.