ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

August 3, 2023

CYBER ESPIONAGE INCIDENT INVOLVING MICROSOFT CLOUD EXPANDS, CHINESE HACKERS MAY HAVE COMPROMISED "HUNDREDS OF THOUSANDS" OF GOVERNMENT EMAIL ACCOUNTS

Scott Ikeda | CPO Magazine | July 26, 2023

A recent cyber espionage campaign by Chinese hackers compromised numerous federal agencies, but was thought to have specifically targeted just a few email accounts at each one. The assessment of the damage from that campaign has now been revised and greatly expanded, with more senior officials and ambassadors confirmed to have been targeted and potentially "hundreds of thousands" of email accounts breached. News of the cyber espionage campaign, which reportedly took place from mid-May to at least mid-June, broke on July 12. At the time the reporting was that quite a few federal agencies had been compromised, but the Chinese hackers were selective about the email accounts they targeted and Commerce Secretary Gina Raimondo was the only high-level official named as a victim. recent Wall Street Journal report has updated that account. The report cites sources "familiar with the matter" in claiming that the number of compromised email accounts is in the hundreds of thousands, and that at least two more high-level officials were among those breached by the cyber espionage campaign: assistant secretary of state for East Asia Daniel Kritenbrink, and Ambassador to China Nicholas Burns.

Read the full article here.

CHINA'S VOLT TYPHOON APT BURROWS DEEPER INTO US CRITICAL INFRASTRUCTURE

Nate Nelson | Dark Reading | July 31, 2023

The U.S. has blocked students from China's military-linked universities but its ally Japan is giving them a The US military was reckoning with two major cyber concerns over the weekend — one the widespread and still unresolved Chinese campaign known as Volt Typhoon targeting military bases, and the other an insider breach affecting Air Force and FBI communications. Biden administration officials have confirmed that Volt Typhoon's malware is much more endemic than previously thought; responders have found it planted inside numerous networks controlling the communications, power, and water feeding US military bases at home and abroad, according to The New York Times. Also concerning, those same networks also touch run of the mill businesses and individuals as well — and investigators are having a hard time assessing the full footprint of the infestation.

Read the full article here.

GERMAN EDUCATION MINISTER RAISES ALARM ABOUT POTENTIAL SPYING RISKS INVOLVING SOME CHINESE STUDENTS

Erudera | July 31, 2023

The German Ministry of Education has recently expressed concerns about the potential threat of scientific espionage from Chinese students studying in Germany under exchange programs. Given these concerns, the German Minister of Education, Bettina Stark-Watzinger, has proposed reviewing student exchange programs with China, Erudera.com reports. In an interview with Mediengruppe Bayern, the Minister called China a systematic rival, adding that the country is becoming a competitor in the field of science and research. *"China is becoming more and more competitive and is a systemic rival in the domain of science and research,"* Stark-Watzinger said. She welcomed the decision of Friedrich-Alexander University (FAU) in Bavaria to not admit any more students who receive funding from the China Scholarship Council (CSC), a non-profit institution within the Chinese Ministry of Education that provides funding to Chinese students to study abroad.

Read the full article here.

STUDENTS ARE 'MAGNETIC TARGETS' FOR ESPIONAGE, HEAD OF MI5 WARNS

Ewan Somerville | The Telegraph | July 22, 2023

In "The Precarious Balance Between Research Openness and Security" (*Issues*, Spring 2023), E. William Colglazier makes an important contribution to the ongoing dialog about science security, and particularly regarding the United States' basic science relationship with China. As a former director of the Department of Energy Office of Science, I agree with his assessment that rushing to engineer and implement even more restrictive top-down controls on basic science collaboration could be counterproductive, especially without a thoughtful analysis of the impact of the actions that already have been taken to thwart nefarious Chinese behavior. In our personal lives, we instinctively understand when a relationship is not mutually beneficial and when we are being taken advantage of even when the rules are vague.

Read the full article here.

FBI WARNS OF ADVERSARIES USING AI IN INFLUENCE CAMPAIGNS, CYBERATTACKS

Martin Matishak | The Record | July 28, 2023

The FBI is paying increased attention to foreign adversaries' attempts to utilize artificial intelligence as part of influence campaigns and other malicious activity, as well as their interest in tainting commercial AI software and stealing aspects of the emerging technology, a senior official said Friday. The two main risks the bureau sees are "model misalignment" — or tilting AI software toward undesirable results during development or deployment — and the direct "misuse of AI" to assist in other operations, said the official, who spoke on the condition of anonymity during a conference call with reporters. The official said foreign actors are "increasingly targeting and collecting against U.S. companies, universities and government research facilities for AI advancements," such as algorithms, data expertise, computing infrastructure and even people.

Read the full article here.

HOW TO PROTECT PRECIOUS IP FROM LAYOFF-RELATED INSIDER THEFT

Walter Pfeffer and Harman Deol | Corporate Compliance Insights | June 7, 2023

With 61% of business leaders reporting that their companies will likely see layoffs in 2023, the reductions in force we've seen this spring may be only the tip of the iceberg. Given that the vast majority of trade secret theft is committed by those within the business — 85% according to one study, supported by the fact that 70% of trade secret cases also include a claim for breach of contract — few will be surprised to see a sharp rise in trade secret misappropriation accompanying these reductions in force. While protecting key confidential and trade secret information is always a balancing act between best practices and the realities of a functioning business, here are some steps that may help companies avoid harm when employees depart. employees cannot take trade secret information if they do not have access to it. Of course, no business can simply lock away its trade secrets and still function. In order for those trade secrets to offer value, some employees must be able to access and use them.

Read the full article here.

SURVEY OF CHINESE ESPIONAGE IN THE UNITED STATES SINCE 2000

Center for strategic and International Studies

This updated survey is based on publicly available information and lists 224 reported instances of Chinese espionage directed at the United States since 2000. It does not include espionage against other countries, against U.S. firms or persons located in China, nor the many cases involving attempts to smuggle controlled items from the U.S. to China (usually munitions or controlled technologies) or the more than 1200 cases of intellectual property theft lawsuits brought by U.S. companies against Chinese entities in either the U.S. or China. The focus is on the illicit acquisition of information by Chinese intelligence officers or their agents and on the increasing number of Chinese covert influence operations. Chinese espionage is undertaken in pursuit of China's strategic objectives. This is a change from the past where commercial motives were often equally important, but commercial espionage by both private and government entities remains a feature of Chinese spying.

Read the full article here.

54% OF AFRICAN STUDENT VISA APPLICATIONS DENIED BY THE US

Wachira Kigotho and Nathan M. Greenfield | University World News | July 27, 2023

African students who apply to study at universities and colleges in the United States experience the highest visa refusal rates of all international students applying to study in the US with more than half of all applicants rejected in 2022. The refusal rate of 54% of student visas in 2022 is up from 44% in 2015, according to a report titled *The Interview of a Lifetime: An analysis of visa denials and international student flows to the US*, from the Presidents' Alliance on Higher Education and Immigration, and Shorelight, two US advocacy groups that promote policies in support of immigrant students. While the refusal rate for African students applying for visas is higher than for students belonging to other geographical categories of visa applicants, it is roughly in line with an across-the-board rise in refusal rates, which suggests that the United States is becoming a less welcoming place to foreign students.

Read the full article here.

REFORMING THE FLAWED PROCESS OF LISTING CHINESE ENTITITES ON A CASE-BY-CASE BASIS

Steve Coonen | China Tech Threat | July 26, 2023

In 2019, the Department of Commerce's Bureau of Industry and Security (BIS) wisely placed Huawei on the Entity List. This action was necessary for making sure the company could not obtain American components it needs to win the 5G race. But Huawei moved fast to protect its interests, quickly spinning off a company called Honor to maintain the flow of U.S. components required to produce 5G mobile devices. A state-owned company, Shenzhen Zhixin New Information Technology, subsequently purchased Honor in 2020, demonstrating the important role that the Chinese government plays in directing strategic technologies such as 5G. During my time serving at the Department of Defense (DOD), I personally pushed for the federal government to add Honor to the Entity List for the same reasons Huawei was. DOD sponsored the review.

Read the full article here.

UNVEILING CHINA'S INTERFERENCE IN U.S. HIGHER ED IS NOT 'ANTI-ASIAN' BIAS

Paul R. Moore | Newsweek | July 25, 2023

Section 117 of the Higher Education Act of 1965 requires colleges and universities to disclose foreign gifts and contracts above $250,000 to the U.S. Department of Education. Because foreign funding may often provide entrée to the research produced by America's higher education system, Congress mandated these disclosures to provide transparency about the role of foreign funding in higher education. Despite its critical purpose, Sec. 117 was largely ignored by colleges and universities and its simple requirements were unevenly enforced under administrations of both political parties, exposing our academic research to tremendous vulnerabilities. In 2019, a bipartisan Senate report confirmed this risk, warning that foreign spending at America's universities is "effectively a black hole" and that as much as 70 percent of U.S. colleges and universities that received foreign gifts and contracts failed to report them.

Read the full article here.

CHINESE ACADEMICS ARE BECOMING A FORCE FOR GOOD GOVERNANCE

Joy Y. Zhang, Sonia Ben Ouagrham-Gormley and Kathleen M. Vogel | Issues in Science and Technology | Summer 2023

At 1:04 a.m. Beijing time on Sunday, March 5, 2023, Chinese bioethicists, legal scholars, and scientists released a consensus statement condemning He Jiankui, the infamous scientist who used the CRISPR gene editing tool to edit the genomes of three babies born in 2018 and 2019. Released from prison in 2022, He quickly began advertising a new—and risky—gene therapy to patients. The March statement denounced He's actions and urged Chinese authorities to be more accountable in their oversight. The statement also protested the censorship and secrecy shrouding He's sentencing and called for more open, public discussion of scientific controversies in China. Global scientists and regulators welcomed the statement, which was released the day before the Third International Summit on Human Genome Editing. It was one of the few times since He's imprisonment in 2019 that the world heard directly from Chinese academics about how controversies involving human genome editing research should (or should not) be handled.

Read the full article here.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE SENIOR ADVISORY GROUP PANEL ON COMMERCIALLY AVAILABLE INFORMATION

Report to the Director of National Intelligence | January 27, 2023

1. (U) There is today a large and growing amount of CAI that is available to the general public, including foreign governments (and their intelligence services) and private-sector entities, as well as the IC. 2. (U) CAI clearly provides intelligence value, whether considered in isolation and/or in combination with other information, and whether reviewed by humans and/or by machines. It also raises significant issues related to privacy and civil liberties. The widespread availability of CAI regarding the activities of large numbers of individuals is a relatively new, rapidly growing, and increasingly significant part of the information environment in which the IC must function. 3. (U) Under IC elements' rules and procedures, CAI (because it is also PAI) is less strictly regulated than other forms of information acquired by the IC. In our view, however, profound changes in the scope and sensitivity of CAI have overtaken traditional understandings, at least as a matter of policy. Today's publicly available CAI is very different in degree and in kind from traditional PAI.

Read the full article here.