ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

July 27, 2022

'BLENDED THREAT': DOJ WARNS OF CHINA, RUSSIA, AND NORTH KOREA ALLYING WITH HACKERS

Jerry Dunleavy | Washington Examiner | July 19, 2022

The Justice Department warned of "alliances" between hacker groups and foreign nations such as China, Russia, and North Korea to form a "blended threat" posing both criminal and national security challenges to the United States. The warning came in DOJ's new Comprehensive Cyber Review report on Tuesday, the result of an internal effort led by Deputy Attorney General Lisa Monaco to prepare DOJ to handle the complicated challenges posed by the sometimes murky cyber landscape. "Criminal actors and nation states are forming alliances of convenience, alliances of opportunity, and sometimes alliances by design," the Justice Department said Tuesday. "Today, some nation states allow this criminal activity to persist without consequence — if not expressly condoning activity within its borders — by acting as a safe harbor for these cyber criminals and turning a blind eye. And the consequences of cyber attacks perpetrated by criminal actors can have national security implications." The Justice Department discussed "cybercrime as means to generate income for malicious foreign governments" and said the department "has seen a rise in hackers with nation-state ties using cybercrime as a way to generate income that can be funneled into other national security threats."

Read the full article here.

UK LABELS LINKEDIN A MAJOR THREAT – SAYS ADVERSARIES TARGETING NATIONAL SECURITY WORKFORCE

Christopher Burgess | ClearanceJobs | July 25, 2022

The United Kingdom's MI5 director general Ken McCallum called out the behavior of the UK's intelligence and military communities' personnel and their use of the social network, LinkedIn. McCallum minced no words noting that personnel were identifying themselves as involved in sensitive classified work and that these disclosures were a breach of government directives. McCallum highlighted how LinkedIn was being used to target UK government and business by the nation's adversaries. The message coming from MI5 mirrors that which has been projected by the U.S. Federal Bureau of Investigation (FBI), who in October 2020, together with the National Counterintelligence and Security Center (NCSC), as part of the national insider threat awareness month, published a 30-minute video, "The Evernight Connection" which detailed the modus operandi used by the Chinese to leverage social networks, like LinkedIn. At that time, NCSC director William Evanina noted, "Social media deception continues to be a popular technique for foreign intelligence services and other hostile actors to glean valuable information from unsuspecting Americans."

Read the full article here.

BILL TO BOOST U.S. CHIP PRODUCTION AND COMPETITION WITH CHINA CLEARS KEY SENATE HURDLE

Kevin Breuninger | CNBC | July 26, 2022

A bipartisan bill to bolster domestic semiconductor manufacturing and boost U.S. competitiveness with China has cleared a key Senate vote, setting it up for final passage in the chamber in the coming days. The so-called cloture vote to break the legislative filibuster was originally set for Monday evening, but had been postponed until Tuesday morning after severe thunderstorms on the East Coast disrupted some senators' travel plans. The vote passed 64-32. Senate Majority Leader Chuck Schumer, D-N.Y., said he hopes lawmakers "can remain on track to finish this legislation ASAP." The package, known as "CHIPS-plus," includes roughly $52 billion in funding for U.S. companies producing computer chips and a provision that offers a tax credit for investment in chip manufacturing. It also provides funding to spur the innovation and development of other U.S. technologies. If it passes the Senate as expected, the House will then take up the legislation. Supporters of the bill hope Congress will pass it and send it to President Joe Biden for his signature before the August recess, which begins in two weeks.

Read the full article here.

MITRE'S INSIDE-R PROTECT GOES DEEP INTO THE BEHAVIOR SIDE OF INSIDER THREATS

Christopher Burgess | CSO | June 23, 2022

Insider threat and risk management programs are the Achilles heel of every corporate and information security program, as many a CISO can attest to. The MITRE Inside-R Protect program is the organization's latest initiative to assist both public and private sector efforts in addressing the insider threat. The Inside-R program's bar for success is high. The focus of Inside-R is on evolving analytic capabilities focused on the behavior of the insider. To that end, MITRE invites the participation of government and private organizations to provide their historical insider incident data to the organization's corpora of information from which findings are derived. While at a nascent stage, the focus on human behavior across a wide swath of historical cases has long been sought and needed by corporate counterespionage programs. I spoke with Dr. Deanna Caputo, MITRE's chief scientist for behavioral sciences and cybersecurity, who emphasizes how the focus of the Insider-R is on the individual's behavior and is non-technical.

Read the full article here.

INTELLIGENCE COMMITTEE MEMBERS WARN US OF BIOWEAPONS TARGETING DNA OF INDIVIDUAL AMERICANS

Anders Hagstrom | Fox News | July 24, 2022

A member of the House Intelligence Committee warned Americans to stay away from DNA testing services as the information could be used to develop bioweapons targeting specific groups of Americans or even individuals. Rep. Jason Crow, D-Colo., made the comments during an appearance at the Aspen Security Forum in Colorado on Friday, saying many Americans are far too willing to give up their DNA information to private companies. "You can't have a discussion about this without talking about privacy and the protection of commercial data because expectations of privacy have degraded over the last 20 years," Crow said "Young folks actually have very little expectation of privacy, that's what the polling and the data show." "People will very rapidly spit into a cup and send it to 23andMe and get really interesting data about their background," he added. Crow, a former Army Ranger, then argued that once a person's DNA is gathered by a private company, that company can then sell it.

Read the full article here.

US PROBES CHINA'S HUAWEI OVER EQUIPMENT NEAR MISSILE SILOS

Alexandra Alper | Reuters | July 21, 2022

The Biden administration is investigating Chinese telecoms equipment maker Huawei over concerns that U.S. cell towers fitted with its gear could capture sensitive information from military bases and missile silos that the company could then transmit to China, two people familiar with the matter said. Authorities are concerned Huawei (HWT.UL) could obtain sensitive data on military drills and the readiness status of bases and personnel via the equipment, one of the people said, requesting anonymity because the investigation is confidential and involves national security. The previously unreported probe was opened by the Commerce Department shortly after Joe Biden took office early last year, the sources said, following the implementation of rules to flesh out a May 2019 executive order that gave the agency the investigative authority. The agency subpoenaed Huawei in April 2021 to learn the company's policy on sharing data with foreign parties that its equipment could capture from cell phones, including messages and geolocational data, according to the 10-page document seen by Reuters. The Commerce Department said it could not "confirm or deny ongoing investigations."

Read the full article here.

HUAWEI SEEKS PROBLEM-SOLVERS WITH 2ND 'YOUNG GENIUS' HIRING DRIVE THIS YEAR

Global Times | July 25, 2022

Chinese technology giant Huawei launched the second round of its genius recruitment program this year on its official WeChat hiring platform on Friday, as it accelerates hiring gifted youth from all over the world amid external pressures and an ongoing US government trade ban. The first such recruitment program was launched on April 25. Under the plan, it doesn't matter where the applicant went to school, as long as they can meet some major requirements relevant to the hi-tech sector. For instance, applicants should have special achievements in mathematics, computing science, physics, intelligent manufacturing, chemistry, semiconductors, materials and other technology-related fields. In the past two years, 26,000 graduates joined Huawei, including 300 gifted youth who have contributed to its key business segments, and promoted technological and software innovation, top executives from Huawei revealed at an earnings conference for the 2021 financial results in March. In 2019, Huawei founder and CEO Ren Zhengfei launched the "young genius" program, which gained public attention with the highest annual salary reaching 2 million yuan ($296,000).

Read the full article here.

ARE STEM STUDENTS FROM THE PEOPLE'S REPUBLIC OF CHINA JEOPARDIZING OUR ECONOMIC AND NATIONAL SECURITY?

George Fishman | Center for Immigration Studies | July 25, 2022

The People's Republic of China under Xi Jinping believes that war with the United States is inevitable. Depending on the outcome of Russia's invasion of Ukraine, the risk of armed conflict might come sooner rather than later. A Russian victory might entice the PRC to invade Taiwan, which could very well draw in U.S. troops. The Chinese Communist Party is intently focused on modernizing its military to close the gap between U.S. and Chinese military power, embracing critical and emerging technologies to serve as "assassin's mace" or "silver bullet" technologies. A RAND Corporation analyst has testified that should it succeed: [This would] represent perhaps the most destabilizing geostrategic development of the 21st century. [S]teep advances in the [People's Liberation Army's] PLA's conventional capabilities ... could, for the first time in modern history, pit the United States against a militarily superior adversary.

Read the full article here.

FOREIGN ACADEMICS IN CHINA

Yuzhuo Cai, Andrea Braun Střelcová, Giulio Marini, Futao Huang, and Xin Xu | Boston College Center for International Higher Education | July 11, 2022

This article examines the experience of international academics in mainland China. The emerging trend of foreign academics moving into long-term, full-time positions in Chinese universities is an underreported phenomenon in research. This article discusses the following questions: Who are the foreign academics in China? What motivates them to go and work there? What are their expected roles in local academia? Are they satisfied with their jobs? Are they going to stay in China? A major global science and technology player, mainland China has also become a destination for international academics. In this regard, the Chinese government's policy has shifted from primarily encouraging overseas Chinese to return to also attracting foreign-born academics to China. Over recent years, the composition of the latter group has evolved. The "old" cohort in this category consisted mainly of university (language) teachers, short-term academic visitors, part-time-post holders and honorary affiliates, trailing spouses, or Chinese returnees.

Read the full article here.

SAFEGUARDING OUR FUTURE - PROTECT YOUR ORGANIZATION'S CROWN JEWELS

National Counterintelligence and Security Center | June 25, 2020

Foreign powers use trusted insiders (employees, researchers, and contractors) or substantial financial investment to gain access to your company's most valuable data. Impact includes: theft of proprietary data, critical technology, and research, compromise of your networks and supply chain, loss of your company's competitive advantage or organizational reputation, significant financial loss, and unforeseen legal liabilities.

Read the full article here.

PROTECTING YOUR ORGANIZATION'S SECRETS – SAFEGUARDING SENSITIVE AND PROPRIETARY INFORMATION FROM FOREIGN ADVERSARIES AND COMPETITORS

National Counterintelligence and Security Center | January 3, 2019

You have access to facilities and computer networks, as well as sensitive information, resources, technologies, research and other data that our foreign adversaries and competitors desperately want. Our adversaries and competitors are interested in you because you have connections and access. You also have social media accounts. A work and/or personal smartphone. Social and professional networks include others in sensitive positions. You may travel, both domestically and abroad. These are all potential vulnerabilities. Foreign adversaries and competitors are actively seeking information that is vital to our national and economic security, U.S. global competitiveness, and your organization's mission. This includes: Sensitive or proprietary financial, trade, or economic policy information; Pioneering research and development; Emerging technologies; Sector-specific information, including commerce, transportation, agriculture, health, homeland security, energy, and communications.

Read the full article here.