ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

May 12, 2021

DARKSIDE RANSOMWARE: BEST PRACTICES FOR PREVENTING BUSINESS DISRUPTION FROM RANSOMWARE ATTACKS

U.S. Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency | May 11, 2021

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are aware of a ransomware attack affecting a critical infrastructure (CI) entity—a pipeline company—in the United States. Malicious cyber actors deployed DarkSide ransomware against the pipeline company's information technology (IT) network.[1] At this time, there is no indication that the entity's operational technology (OT) networks have been directly affected by the ransomware. CISA and FBI urge CI asset owners and operators to adopt a heightened state of awareness and implement the recommendations listed in the Mitigations section of this Joint Cybersecurity Advisory, including implementing robust network segmentation between IT and OT networks; regularly testing manual controls; and ensuring that backups are implemented, regularly tested, and isolated from network connections. These mitigations will help CI owners and operators improve their entity's functional resilience by reducing their vulnerability to ransomware and the risk of severe business degradation if impacted by ransomware.

Read the full article here.

PORTMAN, RUBIO & COLLEAGUES OPPOSE PROPOSED DOJ AMNESTY PROGRAM FOR RESEARCHERS WHO FAILED TO DISCLOSE FOREIGN SUPPORT IN SECURING FEDERAL GRANTS

U.S. Senate Committee on Homeland Security and Governmental Affairs | May 6, 2021

Today, U.S. Senators Rob Portman (R-OH), Ranking Member of the Senate Homeland Security and Governmental Affairs Committee, Marco Rubio (R-FL), John Cornyn (R-TX), Tom Cotton (R-AR), Susan Collins (R-ME), Ben Sasse (R-NE), Todd Young (R-IN) and Chuck Grassley (R-IA) sent a letter to U.S. Attorney General Merrick Garland opposing the reported U.S. Department of Justice (DOJ) amnesty program to allow U.S.-based academics to disclose past foreign funding without fear of prosecution for their disclosures. Last year, Senators Portman, Tom Carper (D-DE), and Rubio introduced the bipartisan Safeguarding American Innovation Act to ensure that the federal government is taking decisive action to safeguard American innovation.

Read the full article here.

HOW CHINA TURNED A PRIZE-WINNING IPHONE HACK AGAINST THE UYGHURS

Patrick Howell O'Neill | MIT Technology Review | May 6, 2021

In March 2017, a group of hackers from China arrived in Vancouver with one goal: Find hidden weak spots inside the world's most popular technologies. Google's Chrome browser, Microsoft's Windows operating system, and Apple's iPhones were all in the crosshairs. But no one was breaking the law. These were just some of the people taking part in Pwn2Own, one of the world's most prestigious hacking competitions. It was the 10th anniversary for Pwn2Own, a contest that draws elite hackers from around the globe with the lure of big cash prizes if they manage to exploit previously undiscovered software vulnerabilities, known as "zero-days." Once a flaw is found, the details are handed over to the companies involved, giving them time to fix it. The hacker, meanwhile, walks away with a financial reward and eternal bragging rights. For years, Chinese hackers were the most dominant forces at events like Pwn2Own, earning millions of dollars in prizes and establishing themselves among the elite. But in 2017, that all stopped.

Read the full article here.

CHINA-BACKED CONFUCIUS INSTITUTES FACE CLOSURE UNDER VETO LAWS

Lisa Visentin | WA Today | May 10, 2021

Australian universities face having their controversial Confucius Institutes shut down within months, with the University of Sydney among the first to submit contracts for scrutiny under the Commonwealth's foreign veto scheme. At least one centre - RMIT University's Chinese Medicine Confucius Institute - will close this year, with the university saying it would cease operations due to budget pressures caused by COVID-19. The institutes, which are hosted by 13 Australian universities in partnership with Chinese universities, have come under scrutiny from the federal government amid concerns they function as a plank of the Chinese Communist Party's propaganda effort. Foreign Minister Marise Payne last month warned "further decisions" were forthcoming as she exercised new veto powers to terminate Victoria's controversial Belt and Road agreement with China, as well as two education agreements made by the state government - one with Iran and one with Syria.

Read the full article here.

GOP REP. BARR TO PROPOSE BILL TO EQUIP FBI WITH RESOURCES TO COMBAT CCP 'ESPIONAGE,' 'THEFT' AT UNIVERSITIES

Brooke Singman | Fox News | May 7, 2021

Republican Rep. Andy Barr is expected to introduce a bill Friday that would create an FBI initiative to root out Chinese Communist Party espionage and theft at higher education institutions in the U.S., Fox News has learned. Fox News first obtained a copy of Barr's, R-Ky., bill, titled the "Higher Education Research Protection Act of 2021." The FBI's Office of Private Sector already exists within the bureau and is tasked with investigating higher education espionage, but Barr's office said the FBI does not have the resources to pull agents from different missions to focus solely on this issue. The bill creates 56 new FBI agent slots under the purview of the Office of the Private Sector—all of whom would directly report to the assistant FBI director, and would be dedicated to investigating and carrying out the mission. If approved, the bill would direct the assistant FBI director to "investigate and report" to the director of the FBI "any suspected incidents of individuals participating in federally funded research as agents of a foreign government in institutions of higher education and National Academies."

Read the full article here.

CHINA'S TECH HUB SHENZHEN TO INVEST US$108 BILLION IN R&D OVER 5 YEARS

Guo Rui | South China Morning Post | May 7, 2021

Shenzhen is set to invest more than 700 billion yuan (US$108 billion) in hi-tech research and development over the next five years as it seeks to reinforce its position as China's innovation powerhouse. Speaking at the city's annual party congress at the end of last month, Shenzhen's Communist Party chief Wang Weizhong said that over the 2021-25 plan period, 5 per cent of GDP would be allocated to investment in R&D to support innovation and breakthroughs in core technologies. The city reported a gross domestic product of 2.8 trillion yuan in 2020, but the government has set a target to increase that to 4 trillion yuan by 2025. Local media reports quoted Wang as saying that artificial intelligence, 6G, quantum technology, driverless vehicles, intelligent networks and other "frontier areas" would be the focus of Shenzhen's investment plans, while the value of its digital economy would account for more than 31 per cent of GDP by 2025.

Read the full article here.

CHINA'S STI OPERATIONS: MONITORING FOREIGN SCIENCE AND TECHNOLOGY THROUGH OPEN SOURCES

William Hannas and Huey-Meei Chang | Center for Security and Emerging Technology | January 2021

Open source intelligence (OSINT) and science and technology intelligence (STI) are realized differently in the United States and China, China putting greater value on both. In the United States' understanding, OSINT "enables" classified reporting, while in China it is the intelligence of first resort. This contrast extends to STI which has a lower priority in the U.S. system, whereas China and its top leaders personally lavish great attention on STI and rely on it for national decisions. Establishing a "National S&T Analysis Center" within the U.S. government could help to address these challenges.

Read the full article here.

SENATORS WARN US JUSTICE DEPARTMENT NOT TO GIVE AMNESTY TO ACADEMICS WHO DIDN'T DISCLOSE FOREIGN FUNDING

Owen Churchill | US-China Relations | May 7, 2021

A group of US Republican senators has called on the Department of Justice not to proceed with a plan to offer amnesty to researchers who come forward about previously undisclosed foreign funding, saying it would undercut efforts to protect "long-term national interests". First reported in January by The Wall Street Journal, the Justice Department's programme would enable US academics to declare prior foreign financial assistance without fear of punishment as part of an effort to assess the scale of overseas funding. The proposal comes as the Justice Department faces growing scrutiny of its China Initiative, a prosecutorial strategy initiated by the Trump administration to protect US intellectual capital. Critics say it has fuelled racial profiling of Chinese and Chinese-American scholars and harmed international academic collaboration. "This is a complex problem, but an amnesty program rewarding individuals who broke federal law to steal US taxpayer-funded research is simply not the answer," eight Republican senators wrote in a letter to US Attorney General Merrick Garland on Wednesday.

Read the full article here.

CHINA ON CAMPUS: HOW THE DOJ HAS BATTLED 'NONTRADITIONAL ESPIONAGE'

Jerry Dunleavy | Washington Examiner | May 5, 2021

The Justice Department's China Initiative is shining the spotlight on the Chinese Communist Party's coordinated and multifaceted efforts to steal research and technology from academic institutions across the country, with prosecutors mounting aggressive efforts over the past few years to crack down on Chinese malign influence at U.S. universities. Attorney General Merrick Garland appeared before the House Appropriations Committee on Tuesday and was pressed on what the DOJ was doing to counter China, especially with regard to the Chinese government's massive theft of intellectual property at public and private institutions. "Well, within the last month or so, the intelligence community has identified China as a threat ... with respect to espionage, with respect to theft of intellectual property, so the FBI is working very hard on these issues," Garland replied.

Read the full article here.

NO STRINGS ATTACHED?

Mick Zais and Reed Rubinstein | Inside Higher Ed | May 6, 2021

Vera Zhou is a student at the University of Washington. During what was to have been a one-week trip to visit her father in Xinjiang, China, in 2017, she was arrested for using a virtual private network to access her homework online. She was interrogated all night, placed in a remote "re-education" prison for six months and kept under house arrest for another 18 months. Zhou's terrified mother, a U.S. citizen and resident of Washington, worked with human rights advocates and the U.S. Department of State to secure her release. With courage and persistence, Zhou has resumed her studies at the university, but her full story reveals continuing scars and troubling details. The University of Washington had no desire to see any harm befall Zhou or, surely, any of its students. Nobody doubts that. But for the last decade, the Chinese Communist Party has pursued an intentional practice of crafting relationships with influential institutions like the university, particularly where they are on the cutting edge of engineering or located adjacent to technology development hubs -- as UW certainly is.

Read the full article here.

INTRUSION TRUTH DETAILS WORK OF SUSPECTED CHINESE HACKERS WHO ARE UNDER INDICTMENT IN US

Sean Lyngaas | Cyber Scoop | May 6, 2021

Intrusion Truth, a mysterious group known for exposing suspected Chinese cyber-espionage operations, on Thursday published a new investigation that traced front companies allegedly used by two Chinese men whom a U.S. grand jury indicted last year. The findings shed light on a dynamic that U.S. law enforcement officials say is increasingly common: foreign intelligence services' use of front companies to try to conceal their hacking operations. The details also come at a time when Biden administration officials are dealing with the fallout of another suspected Chinese hacking campaign in which attackers leveraged widely used Microsoft software. The Justice Department has alleged that the two suspects, Li Xiaoyu and Dong Jiazhi, met at university before embarking on a decade of malicious cyber activity, sometimes for personal financial gain and other times on behalf of the Ministry of State Security, China's civilian intelligence agency. In some cases, the men allegedly probed the networks of U.S. firms working on a coronavirus vaccine. U.S. prosecutors have accused the men of stealing hundreds of millions of dollars in trade secrets and other data.

Read the full article here.

DOUBTS LINGER OVER BIDEN'S EDUCATION DEPARTMENT CONTINUING TRUMP-ERA CHINA INVESTIGATIONS

Jerry Dunleavy | Washington Examiner | May 6, 2021

The Education Department is declining to weigh in on investigations into foreign funding on campuses initiated by the Trump administration and won't comment on possible future inquiries either after Trump officials increased pressure on China. The United States has ramped up its efforts in recent years to confront China, including the Justice Department's China Initiative, the blacklisting of Chinese telecommunications company Huawei and other CCP-linked entities as national security threats, and a crackdown on Confucius Institutes, the Thousand Talents Program, and other Chinese influence operations. Thus far, though, the Biden Education Department has been largely mum on the issue. Miguel Cardona, President Joe Biden's education secretary, did not bring up, nor was he asked about, Chinese influence operations during his February confirmation hearing, nor during a budget request appearance before the House on Wednesday.

Read the full article here.

CONGRESS ADVANCES LEGISLATION TARGETING U.S.-CHINA COMPETITION AND HIGH-TECH INVESTMENT

Timothy Brightbill, Nova Daly, Hon. Nazak Nikakhtar, and Adam Teslik | JD Supra | April 26, 2021

On April 21, 2021, Congress took action on two bills aimed at strengthening U.S. competitiveness vis-à-vis the People's Republic of China (PRC or China). First, the Senate Foreign Relations Committee voted to advance the Strategic Competition Act of 2021. Second, Senators Chuck Schumer (D-NY) and Todd Young (R-IN), along with Representatives Ro Khanna (D-CA) and Mike Gallagher (R-WI), introduced the Endless Frontier Act. These bills are part of a broader wave of legislative action in Congress responding to Chinese policies that the U.S. government recognizes as posing threats to U.S. national and economic security. The 281-page Strategic Competition Act presents findings that "the PRC has chosen to pursue state-led, mercantilist economic policies, an increasingly authoritarian governance model . . . and an aggressive and assertive foreign policy."

Read the full article here.

CHINA ON CAMPUS: CONFUCIUS INSTITUTES COLLAPSE NATIONWIDE

Jerry Dunleavy | Washington Examiner | May 4, 2021

The Chinese Communist Party-linked Confucius Institutes are collapsing in the United States, falling from over 100 to just over a couple dozen in a few years thanks to pressure from the Trump administration and growing concern within the U.S. government about the challenge posed by Chinese influence at U.S. colleges and universities. The U.S. government considers Confucius Institutes to be part of the Chinese government's numerous and varied foreign influence operations, and the Trump administration increased pressure against the groups, including labeling their center in the nation's capital to be a "foreign mission" of Beijing. While the number of Confucius Institutes in the U.S. numbered over 100 just a few years ago, they have now dwindled to what the State Department says is just 27 university sponsors currently operating exchange visitor programs affiliated with the Chinese organization, though that might not fully capture a number of other Confucius Institute partnerships the group has in the U.S. Perhaps the starkest example of the downfall of Confucius Institutes on U.S. campuses is the previously unreported revelation that Columbia University, the only Ivy League school which had such an institute, recently, and quietly, closed the institute after nearly a decade of operation.

Read the full article here.

UNIVERSITY OF ALBERTA TO WORK WITH 'ALL LEVELS OF GOVERNMENT' TO CURTAIL RESEARCH TIES WITH CHINA

Isaac Teo | The Epoch Times | May 5, 2021

The University of Alberta says it's willing to work with all levels of government after a report revealed that the university had been collaborating with China in critical research areas that could undermine Canada's national security. "A consistent national response on security matters and international engagement is necessary and we are fully committed to working with all levels of government to ensure that Canada's core security interests are protected and advanced," said Walter Dixon, the university's interim vice-president of research and innovation, in a statement on Tuesday. "We have asked the federal government for further direction about international collaborations." Dixon added that the university is looking forward to Ottawa's guidelines on national security considerations related to the evaluation and funding of research partnerships, which are expected in June.

Read the full article here.

SENATE HELP COMMITTEE HOLDS HEARING ON FOREIGN INFLUENCE IN BIOMEDICAL RESEARCH

Christa Wagner | AAMC | April 23, 2021

NIH Deputy Director for Extramural Research Michael Lauer, MD, testified on the NIH's efforts to combat foreign influence in biomedical research in an April 22 hearing before the Senate Health, Education, Labor, and Pensions (HELP) Committee. Lauer testified that the NIH's main areas of concern regarding foreign government influence on the NIH research enterprise are the failure of researchers to disclose outside funding from other organizations or foreign governments, "diversion of proprietary information included in grant applications or produced by NIH-supported biomedical research to other entities," and a breach of confidentiality in the peer review system. "As of April 2021, we have contacted more than 90 awardee institutions regarding concerns involving over 200 scientists," he stated. Lauer reviewed the NIH's actions to prevent these security issues, which include proactively addressing the research community, working with other federal research agencies through the Office of Science and Technology Policy to coordinate resources for grantees, and collaborating with national security agencies such as the Federal Bureau of Investigation and the Department of Health and Human Services (HHS) Office of National Security (ONS) and Office of Inspector General.

Read the full article here.

US PHYSICS LAB FERMILAB EXPOSES PROPRIETARY DATA FOR ALL TO SEE

ARS Technica | May 6, 2021

Multiple unsecured entry points allowed researchers to access data belonging to Fermilab, a national particle physics and accelerator lab supported by the Department of Energy. This week, security researchers Robert Willis, John Jackson, and Jackson Henry of the Sakura Samurai ethical hacking group have shared details on how they were able to get their hands on sensitive systems and data hosted at Fermilab. After enumerating and peeking inside the fnal.gov subdomains using commonly available tools like amass, dirsearch, and nmap, the researchers discovered open directories, open ports, and unsecured services that attackers could have used to extract proprietary data. The server exposed configuration data for one of Fermilab's experiments called "NoVa," which concerns studying the purpose of neutrinos in the evolution of the cosmos.

Read the full article here.

SIUC MATH PROFESSOR INDICTED IN FEDERAL COURT FOR ALLEGED GRANT FRAUD

Carolyn P. Smith | Belleville lNews-Democrat | April 23, 2021

A mathematics professor and researcher at Southern Illinois University at Carbondale was indicted in a federal court, accused of concealing support he was receiving from the Chinese government in order to obtain grant money in the U.S. According to charging documents filed in the U.S. Court for the Southern District of Illinois, Mingquing Xiao, 59, of Makanda obtained a $151,099 federal grant from the National Science Foundation without disclosing his ties to an arm of the Chinese government and a conflicting commitment to Shenzen University. He was charged Wednesday with two counts of wire fraud and a single count of making false statements. Mandating such disclosures may protect research conducted at American universities from being stolen by other global competitors, said Assistant Attorney General John Demers in a release issued by the National Security Division of the U.S. Department of Justice.

Read the full article here.

COMMUNIST CHINESE MILITARY COMPANIES AND SECTION 1237: A PRIMER

Jprdan Brunner | Lawfare Blog | March 22, 2021

In recent months, two Chinese companies have filed lawsuits contesting their designation as "Communist Chinese military companies" (CCMCs) by the Department of Defense. Xiaomi and Luokung Technology have filed proceedings in the U.S. District Court for the District of Columbia against the Defense and Treasury departments for alleged violations of their due process rights. On March 12, Judge Rudolph Contreras of the D.C. District Court granted Xiaomi a preliminary injunction against their designation. These companies have been "blacklisted" under Section 1237 of the Strom Thurmond National Defense Authorization Act (NDAA) for fiscal year 1999, as amended. This post provides background on Section 1237, examines the current state of play, and assesses the ongoing legal battle between the U.S. government and the companies over the CCMC label and its accompanying consequences.

Read the full article here.

RUSSIAN FOREIGN INTELLIGENCE SERVICE (SVR) CYBER OPERATIONS: TRENDS AND BEST PRACTICES FOR NETWORK DEFENDERS

Cybersecurity and Infrastructure Security Agency | April 26, 2021

The Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Cybersecurity and Infrastructure Security Agency (CISA) assess Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and Yttrium—will continue to seek intelligence from U.S. and foreign entities through cyber exploitation, using a range of initial exploitation techniques that vary in sophistication, coupled with stealthy intrusion tradecraft within compromised networks. The SVR primarily targets government networks, think tank and policy analysis organizations, and information technology companies.

Read the full article here.