ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

June 8, 2022

PEOPLE'S REPUBLIC OF CHINA STATE-SPONSORED CYBER ACTORS EXPLOIT NETWORK PROVIDERS AND DEVICES

U.S. Joint Cybersecurity Advisory | June 2022

This joint Cybersecurity Advisory describes the ways in which People's Republic of China (PRC) state-sponsored cyber actors continue to exploit publicly known vulnerabilities in order to establish a broad network of compromised infrastructure. These actors use the network to exploit a wide variety of targets worldwide, including public and private sector organizations. The advisory details the targeting and compromise of major telecommunications companies and network service providers and the top vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—associated with network devices routinely exploited by the cyber actors since 2020. This joint Cybersecurity Advisory was coauthored by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI). It builds on previous NSA, CISA, and FBI reporting to inform federal and state, local, tribal, and territorial (SLTT) government; critical infrastructure (CI), including the Defense Industrial Base (DIB); and private sector organizations about notable trends and persistent tactics, techniques, and procedures (TTPs).

Read the full article here.

BIDEN ADMINISTRATION PLACES TOP CHINESE MILITARY INSTITUTE ON EXPORT BLACKLIST OVER ITS USE OF SURVEILLANCE, 'BRAIN-CONTROL' TECHNOLOGY

Ellen Nakashima and Aaron Schaffer | The Washington Post | December 16, 2021

The Biden administration said Thursday it is adding China's top military medical research institute to an export blacklist in response to concerns about Beijing's use of emerging technologies such as biometrics and "brain-control" weapons in ways that U.S. officials say threaten national security. The Commerce Department added the Academy of Military Medical Sciences and 11 of its research institutes to the Entity List, which bans the export of American technology to the entity unless the exporter receives a government license. The academy and its research institutes focus on using biotechnology to support the Chinese military, officials said. Commerce is also adding more than a dozen Chinese firms to the blacklist, citing their help in modernizing the Chinese military and supporting Iran's weapons program and defense industry. Also on Thursday, the Treasury Department placed eight Chinese companies on a U.S. investment blacklist, saying that the entities support biometric surveillance and tracking of ethnic and religious minorities in China, particularly Uyghur Muslims in the northwestern Xinjiang region.

Read the full article here.

WORLD'S 1ST ANTI-HYPERSONIC SYSTEM? CHINA SAYS IT IS READY WITH AN AI-POWERED DEFENSE AGAINST MACH 5+ MISSILES

Sakshi Tiwari | The EurAsian Times | June 2, 2022

Chinese military researchers claim to have developed Artificial Intelligence (AI) technology that can predict the trajectory of a hypersonic glide missile as it approaches a target at speeds exceeding five times that of sound, South China Morning Post reported. A rocket is used to launch a hypersonic glide vehicle to hit a target. The glide vehicle subsequently separates from the rocket and moves toward its target at a speed of at least Mach 5, or five times the speed of sound. It is extremely difficult to track a hypersonic glide missile due to its unpredictable trajectory and the ability to enter space and re-enter the atmosphere in a very short period. Countries like the US are also relentlessly working on developing air missile defense against hypersonic missiles. The Chinese researchers, however, seem to be several steps ahead of their American counterparts. According to them, a Chinese AI-powered air defense system can predict the potential kill trajectory of an incoming weapon and launch a swift counterattack with a three-minute advance time. The typical missile stays within an 8-kilometer (5-mile) target zone, which is quite small for a weapon that can travel that distance in under two seconds.

Read the full article here.

RESEARCH SECURITY RULES: IS UNIVERSITY AUTONOMY AT RISK?

Jan Petter Myklebust | University World News | June 4, 2022

The Danish Ministry of Higher Education and Science published a report on 25 May which calls for a "paradigm shift" in the Danish approach to international research and innovation and offers practical guidelines for Danish educational and research institutions to "reduce risks and increase the potential for benefits in international research and innovation collaboration". The Danish measures are part of broader efforts by Nordic countries to combat intellectual espionage and information misuse in international research collaborations. While cooperation with countries such as China and Russia tends to be foregrounded as current security threats, most of the measures are designed to be applied more generally. "Danish universities shall in the future follow a set of guidelines when collaborating with international partners to prevent [a situation in which] international researchers in reality are used for espionage or theft of technology for military use," the report said.

Read the full article here.

US INTEL CHIEF: CYBERSECURITY IS ONLY GETTING HARDER

Martin Matishak | The Record | June 6, 2022

Innovation by cyber adversaries and within the commercial spyware sector are among the key aspects making digital security increasingly difficult for the U.S. intelligence community to effectively manage, the nation's spy chief said Monday. "I think cybersecurity is getting harder," Director of National Intelligence Avril Haines said during a keynote address at the RSA Conference. The somber assessment comes as the federal government and the private sector remain on a heightened state of alert about online attacks spiraling out of Russia's invasion of Ukraine and the ever–present threat of digital piracy or assault by China and other malicious actors. Haines admitted that the U.S. has "not figured out how to prevent intrusions of even sophisticated networks… That is a challenge I think that we're going to live with and the reality is we are from an intelligence community perspective." She specifically cited the increased commercial availability of sophisticated offensive tools that "make it harder for us to manage and it makes it easier for other actors to basically obtain tools that then allow them to engage in pretty sophisticated attacks in a variety of ways."

Read the full article here.

HOW DID CHINA BECOME THE WORLD'S NO.1 INTELLECTUAL PROPERTY THIEF?

Teresa Jones | The BL | June 6, 2022

$600 billion, do you have any idea of what one could do with that huge amount of money? In May 2022, Ukrainian President Zelensky estimated that it would take roughly $600 billion to rebuild his country from the pile of debris left after the war, reported The Wall Street Journal. Coincidently, between $225 billion to $600 billion is also the annual cost to the U.S. economy of stolen trade secrets, pirated software, and counterfeiting, not including the full cost of patent infringement, according to an official estimate. Most of these goods are "made in China." "In our assessment, we believe that we're talking about trillions, not billions," Boston-based cybersecurity firm Cybereason CEO Lior Div told CBS News. "The real impact is something we're going to see in five years from now, ten years from now, when we think that we have the upper hand on pharmaceutical, energy, and defense technologies. And we're going to look at China and say, how did they bridge the gap so quickly without the engineers and resources?"

Read the full article here.

THE SURREAL CASE OF A C.I.A. HACKER'S REVENGE

Patrick Radden Keefe | The New Yorker | June 6, 2022

Nestled west of Washington, D.C., amid the bland northern Virginia suburbs, are generic-looking office parks that hide secret government installations in plain sight. Employees in civilian dress get out of their cars, clutching their Starbucks, and disappear into the buildings. To the casual observer, they resemble anonymous corporate drones. In fact, they hold Top Secret clearances and work in defense and intelligence. One of these buildings, at an address that is itself a secret, houses the cyberintelligence division of the Central Intelligence Agency. The facility is surrounded by a high fence and monitored by guards armed with military-grade weapons. When employees enter the building, they must badge in and pass through a full-body turnstile. Inside, on the ninth floor, through another door that requires badge access, is a C.I.A. office with an ostentatiously bland name: the Operations Support Branch. It is the agency's secret hacker unit, in which a cadre of élite engineers create cyberweapons. "O.S.B. was focussed on what we referred to as 'physical-access operations,' " a senior developer from the unit, Jeremy Weber—a pseudonym—explained.

Read the full article here.

ENGINEER WHO FLED CHARGES OF STEALING CHIP TECHNOLOGY IN US NOW THRIVES IN CHINA

Jordan Robertson and Michael Riley | Bloomberg | June 5, 2022

Few companies are better positioned to benefit from the crippling shortage of computer chips than ASML Holding NV, a Dutch manufacturer whose equipment plays an integral role in making the world's most advanced semiconductors. But four lines tucked halfway into an otherwise upbeat, 281-page annual report from February hinted at a potentially incendiary problem. ASML accused a Beijing-based firm, regarded by Chinese officials as one of the country's most promising tech ventures, of potentially stealing its trade secrets. Behind the brief disclosure is an extraordinary multiyear tale of intellectual property theft and a broader threat facing the $556 billion semiconductor industry. In the report, ASML said the Chinese company, Dongfang Jingyuan Electron Ltd., is related to a defunct Silicon Valley firm, Xtal Inc., which ASML sued for intellectual property theft. A 2018 trial in California, which received scant attention at the time, provided more detail. Dongfang and Xtal were essentially the same, created a month apart in 2014 by a former ASML engineer named Zongchang Yu, ASML's attorney told the court.

Read the full article here.

CHINA'S SPIES ARE NOT ALWAYS AS GOOD AS ADVERTISED

The Economist | June 1, 2022

In recent years Western officials have maintained a steady drumbeat of warnings about Chinese spies. In short, the spooks are getting bolder and better. Among other things, they're accused of hacking into Microsoft's Exchange email service, stealing Western defence and commercial secrets, harassing Chinese dissidents overseas and bugging the headquarters of the African Union (all of which China denies). Yet, when confronted by overwhelming evidence that Russia was about to invade Ukraine, China's spies appear to have dropped the ball. Whatever Vladimir Putin told Xi Jinping when the two presidents met in Beijing on February 4th, China did not seem prepared for Russia's invasion three weeks later. One giveaway was its failure to make plans to evacuate its citizens in Ukraine. China's embassy first advised them to stay at home or fix a Chinese flag "on an obvious place on your car". If Chinese officials had in mind "Wolf Warrior 2", a nationalistic film in which the hero passes the frontlines of an African conflict by raising a Chinese flag, they were disappointed. China's parroting of Russian propaganda has not made it popular in Ukraine.

Read the full article here.

CHINESE STUDENTS MORE RELUCTANT TO STUDY ABROAD POST-COVID

Joshua Ka-ho Mok | University World News | June 4, 2022

The spread of the COVID-19 pandemic has dramatically changed the landscape of global higher education by decreasing international mobility and fostering the emergence of new study abroad destinations. Although a sharp increase in international student mobility has occurred over the past two decades, the overall percentage is rather low, with only 2% of the world's total students involved. Furthermore, that mobility is mainly in a single direction, mostly from the Global South to the Global North. The outbreak of the pandemic has dramatically changed the landscape. International student mobility has been facing unprecedented challenges caused by the pandemic. With travel restrictions and closed borders, many students cancelled or changed their overseas education plans, reshaping the landscape of international higher education. Universities in Anglophone countries have been more likely to be influenced because they are more financially dependent on fee-paying international students and receive the lion's share of the world's internationally mobile students.

Read the full article here.

THE HACKER GOLD RUSH THAT'S POISED TO ECLIPSE RANSOMWARE

Lily Hay Newman | Wired | June 5, 2022

Ransomware attacks, including those of the massively disruptive and dangerous variety, have proved difficult to combat comprehensively. Hospitals, government agencies, schools, and even critical infrastructure companies continue to face debilitating attacks and large ransom demands from hackers. But as governments around the world and law enforcement in the United States have grown serious about cracking down on ransomware and have started to make some progress, researchers are trying to stay a step ahead of attackers and anticipate where ransomware gangs may turn next if their main hustle becomes impractical. At the RSA security conference in San Francisco on Monday, longtime digital scams researcher Crane Hassold will present findings that warn it would be logical for ransomware actors to eventually convert their operations to business email compromise (BEC) attacks as ransomware becomes less profitable or carries a higher risk for attackers. In the US, the Federal Bureau of Investigation has repeatedly found that total money stolen in BEC scams far exceeds that pilfered in ransomware attacks—though ransomware attacks can be more visible and cause more disruption and associated losses.

Read the full article here.

US: CHINESE GOVT HACKERS BREACHED TELCOS TO SNOOP ON NETWORK TRAFFIC

Sergiu Gatlan | Bleeping Computer | June 7, 2022

Several US federal agencies today revealed that Chinese-backed threat actors have targeted and compromised major telecommunications companies and network service providers to steal credentials and harvest data. As the NSA, CISA, and the FBI said in a joint cybersecurity advisory published on Tuesday, Chinese hacking groups have exploited publicly known vulnerabilities to breach anything from unpatched small office/home office (SOHO) routers to medium and even large enterprise networks. Once compromised, the threat actors used the devices as part of their own attack infrastructure as command-and-control servers and proxy systems they could use to breach more networks.

Read the full article here.

NEW SEC CYBERSECURITY RULES FOCUS ON BOARD ACCOUNTABILITY

James Turgal | NACD BoardTalk | June 7, 2022

Gone are the days when cybersecurity was just an information technology (IT) problem. Cyber risk is central to business risk, making it a board-level issue. For the first time, a proposed rule set from the US Securities and Exchange Commission (SEC) will require virtually all commission registrants to provide a series of cybersecurity disclosures within mandated annual and quarterly reporting. This decision is a nod to the importance of cybersecurity standards and what investors need to know to make an informed decision. There have been several cybersecurity-centered proposals for registered investment advisors and funds of late, including the Cybersecurity Disclosure Act of 2017, the Strengthening of America Cybersecurity Act in March 2022, and the Better Cybercrime Metrics Act that just passed last month.

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.[1]

Read the full article here.