ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

August 12, 2020

HOOVER INSTITUTION PUBLISHES GLOBAL ENGAGEMENT: RETHINKING RISK IN THE RESEARCH ENTERPRISE

Hoover Institution | August 5, 2020

The Hoover Institution has released a new report that details the challenges that the US government and American laboratories and universities face in their research engagements with counterparts in the People's Republic of China (PRC). The report also offers practical recommendations to US policy makers and principals for managing the risks that these partnerships pose. Global Engagement: Rethinking Risk in the Research Enterprise is edited by Glenn Tiffert, Hoover Institution visiting fellow and expert on the history of modern China. Tiffert manages Hoover's projects on Taiwan in the Indo-Pacific Region and on China's Global Sharp Power, both chaired by senior fellow Larry Diamond. The report is an initiative of the latter project, which aims to track the PRC's efforts to subvert free and open societies and to control global narratives in favor of the ideals and ambitions of China's Communist Party.

Read the full report here.

PILLARS OF RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM

U.S. Department of State Global Engagement Center Special Report | August 2020

As the U.S. Government's dedicated center for countering foreign disinformation and propaganda, the Global Engagement Center (GEC) at the U.S. Department of State has a mandate to expose and counter threats from malign actors that utilize these tactics. In this field, Russia continues to be a leading threat. The Department works with interagency and global partners to meet this challenge, with the GEC playing a key role in coordinating efforts and helping lead a global response. A central part of this effort is exposing Russia's tactics so that partner and allied governments, civil society organizations, academia, the press, and the international public can conduct further analysis of their own and thereby increase collective resilience to disinformation and propaganda. In line with that goal, this report draws on publicly available reporting to provide an overview of Russia's disinformation and propaganda ecosystem. Russia's disinformation and propaganda ecosystem is the collection of official, proxy, and unattributed communication channels and platforms that Russia uses to create and amplify false narratives.

Read the full report here.

INFORMATION ABOUT THE DEPARTMENT OF JUSTICE'S CHINA INITIATIVE AND A COMPILATION OF CHINA-RELATED PROSECUTIONS SINCE 2018

U.S. Department of Justice | August 4, 2020

About 80 percent of all economic espionage prosecutions brought by the U.S. Department of Justice (DOJ) allege conduct that would benefit the Chinese state, and there is at least some nexus to China in around 60 percent of all trade secret theft cases. The Department of Justice's China Initiative reflects the strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. The Initiative was launched against the background of previous findings by the Administration concerning China's practices. In March 2018, the Office of the U.S. Trade Representative announced the results of an investigation of China's trade practices under Section 301 of the Trade Act of 1974. It concluded, among other things, that a combination of China's practices are unreasonable, including its outbound investment policies and sponsorship of unauthorized computer intrusions, and that "[a] range of tools may be appropriate to address these serious matters."

Read the full article here.

IC LEADER DETAILS PRESENT AND FUTURE CYBER THREATS

Dwight Weingarten | Meri Talk | August 11, 2020

Days after the director of the National Counterintelligence and Security Center (NCSC) announced the ongoing efforts of foreign nations to interfere in U.S. elections, he offered five additional areas as the present and future of cybersecurity. William Evanina, the director of NCSC, pointed to the cyber challenges of defending COVID-19 research, economic espionage, protecting critical infrastructure, supply chain safety, and traditional espionage as the threats apart from elections. "Let's not hide the fact that many nation-states around the world are attacking us on a daily basis with respect to our development of a vaccine," said Evanina, in recorded remarks during the FCW Cybersecurity Workshop on August 11. Last month, cybersecurity agencies in the U.S., United Kingdom, and Canada issued a joint advisory that said a Russia-linked group was targeting COVID-19 research.

Read the full article here.

TRUMP TARGETS WECHAT AND TIKTOK, IN SHARP ESCALATION WITH CHINA

Ana Swanson, Mike Isaac, and Paul Mozur | The New York Times | August 6, 2020

The Trump administration has announced sweeping restrictions on two popular Chinese social media networks, TikTok and WeChat, a sharp escalation of its confrontation with China that is likely to be met with retaliation. Two executive orders, released late Thursday and taking effect in 45 days, cited national security concerns to bar any transactions with WeChat or TikTok by any person or involving any property subject to the jurisdiction of the United States. The order essentially sets a 45-day deadline for an acquisition of TikTok, which is in talks to be acquired by Microsoft. Tensions between the United States and China have already escalated to levels not seen in decades over rifts in geopolitics, technology and trade. In recent months, Trump administration officials have challenged China on its crackdown in Hong Kong, its territorial claims in the South China Sea and its efforts to produce global tech champions. The campaign has been provoked in part by China's more assertive posture, but also President Trump's desire to convince voters that he is tough on China as the election approaches.

Read the full article here.

CHINESE GOVERNMENT-PAID SCIENTISTS PLEAD GUILTY TO STEALING RESEARCH FROM AN AMERICAN CHILDREN'S HOSPITAL

Bonnie Girard | The Diplomat | August 8, 2020

A Chinese researcher pled guilty on July 30 for conspiring to steal proprietary trade secrets from a hospital research institute in the United States, and for the wire fraud that accompanied the theft. This was no ordinary hospital research facility, either. The victim was no less than the Nationwide Children's Hospital's Research Institute. The hospital earned a place on the Honor Roll in U.S. News and World Report's latest rankings of similar hospitals in America. The FBI called the theft "another example of economic malfeasance related to the People's Republic of China." It added that "far from being an isolated incident, we see the PRC implicated in around 60 percent of all trade secret theft cases." The case illustrates one of the worst sides of the Chinese Communist Party's campaign to empty out the intellectual property coffers of not only the United States, but anywhere in the world where a hard-won nugget of scientific or engineering value may lurk.

Read the full article here.

CHINESE ESPIONAGE: A FAR-REACHING AND LONG-LASTING THREAT

William Tucker | In Homeland Security | August 5, 2020

Speaking at a recent event hosted by the Hudson Institute, FBI Director Christopher Wray discussed Chinese espionage, the threat it poses to the U.S. economy and national security. Director Wray characterized the theft of U.S. intellectual property as "one of the largest transfers of wealth in human history." Some U.S. businesses have closed their doors and many Americans have lost their jobs because of this effort by the Chinese. Overall, the losses to U.S. businesses come to over a trillion dollars. To place this amount in perspective, consider the Sinovel espionage case. American Superconductor, a U.S. company, had its proprietary software stolen by Sinovel, a Chinese wind turbine manufacturer. The theft cost the U.S. company $800 million, forcing it to lay off 600 of its 900 employers. It also cost investors one billion dollars. The Sinovel case is but one example. Director Wray remarked, "We've now reached the point where the FBI is opening a new China-related counterintelligence case about every 10 hours.

Read the full article here.

UNIVERSITIES CRACK DOOR FOR UNRELENTING IP THEFT, CYBER THREATS AGAINST DEFENSE SECTOR

Travis Smalls and Mitchell Simmons | Homeland Security Today | August 5, 2020

The U.S. government routinely collaborates with universities to research and pursue innovative technological and other advancements; however, the cultural differences between the U.S. government and academia create vulnerabilities. The U.S. government operates on a somewhat restrictive platform, while universities champion transparency, openness, and free exchange of ideas amongst researchers. One of the major challenges in this collaboration is the targeting of IP within the U.S. defense sector by adversarial nations such as China, whose goal is to challenge or supplant U.S. dominance. The U.S. defense sector is the largest in the world and is one of the 16 critical infrastructures defined by the Department of Homeland Security (DHS). According to DHS, the U.S. Defense Industrial Base (DIB) sector is the worldwide industrial complex that enables research and development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements; the sector consists of approximately 100,000 companies.

Read the full article here.

NATIONAL INSIDER THREAT AWARENESS MONTH

National Counterintelligence and Security Center

Participating in Insider Threat Awareness Month 2020 can help your program detect, deter, and mitigate insider threats by increasing awareness and promoting reporting. Insider threat awareness is not about curtailing protected free speech or suppressing legitimate whistleblowing; it is about preventing the exploitation of authorized access to cause harm to an organization or its resources. It is vital that we prevent these actions and safeguard national security, while protecting privacy and civil liberties. There are many ways to get involved. This website will help you identify a variety of activities and engagements available to your organization. From utilizing the provided awareness materials to hosting an Insider Threat Awareness day, actions both small and large will help bring attention to the counter-insider threat mission. We look forward to partnering with you during this important campaign. Remember, we all speak louder with one voice.

Visit the Web site here.

SPECIAL REPORT: COVID OPENS NEW DOORS FOR CHINA'S GENE GIANT

Kirsty Needham | Reuters | August 5, 2020

As countries scramble to test for the novel coronavirus, a Chinese company has become a go-to name around the world. BGI Group, described in one 2015 study as "Goliath" in the fast-growing field of genomics research, is using an opening created by the pandemic to expand its footprint globally. In the past six months, it says it has sold 35 million rapid COVID-19 testing kits to 180 countries and built 58 labs in 18 countries. Some of the equipment has been donated by BGI's philanthropic arm, promoted by China's embassies in an extension of China's virus diplomacy. But as well as test kits, the company is distributing gene-sequencing technology that U.S. security officials say could threaten national security. This is a sensitive area globally. Sequencers are used to analyse genetic material, and can unlock powerful personal information. In science journals and online, BGI is calling on international health researchers to send in virus data generated on its equipment, as well as patient samples that have tested positive for COVID-19, to be shared publicly via China's government-funded National GeneBank.

Read the full article here.

PRIME FUTURE 014: FIVE WAYS LAND GRANTS CAN SET THE PACE IN A POST-COVID AGRICULTURE INDUSTRY

Janette Barnard | Prime Future | July 25, 2020

The world is moving fast. Universities seem to move…less fast. With universities making plans for education delivery in the upcoming academic year, it raises some interesting questions about enrollment, revenue, and sustainability of the current model. The question for universities is not how they will serve students this fall. It's how they will serve their purpose in 5 years. To be frank, will they serve their purpose in 5 years? Because of their historical importance to the agriculture industry in educating workforce and conducting research, I'm most interested in the future of land grant institutions. I hold degrees from two land grant schools (University of Arizona and Texas A&M) so I'm a product of the system signed into law by President Lincoln in 1862, and a big fan.

Read the full article here.

ANNOUNCING THE EXPANSION OF THE CLEAN NETWORK TO SAFEGUARD AMERICA'S ASSETS

Michael R. Pompeo, Secretary of State | August 5, 2020

The Clean Network program is the Trump Administration's comprehensive approach to guarding our citizens' privacy and our companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party (CCP). Today, I am announcing the launch of five new lines of effort to protect America's critical telecommunications and technology infrastructure. These programs are rooted in internationally accepted digital trust standards and built upon the 5G Clean Path initiative, announced on April 29, 2020, to secure data traveling on 5G networks into U.S. diplomatic facilities overseas and within the United States.

Read the full statement here.

WATCH: FBI DIRECTOR CHRIS WRAY WARNS AMERICANS ON 3 THINGS THEY NEED TO KNOW ABOUT CHINA

The Daily Wire | August 8, 2020

FBI Director Christopher Wray recently delivered a speech in which he warned Americans about three things that they need to know about what the Chinese Communist Party is trying to do to the United States. In remarks given at the Hudson Institute last month, Wray warned that the Chinese Communist Party was working to become the world's only superpower by "any means necessary." "If you are an American adult, it is more likely than not that China has stolen your personal data," Wray said. "We've now reached the point where the FBI is opening a new China-related counterintelligence case about every 10 hours. Of the nearly 5,000 active FBI counterintelligence cases currently underway across the country, almost half are all related to China. And at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research."

Read the full article here.

FROM COMPETITION TO CONFRONTATION WITH CHINA: THE MAJOR SHIFT IN U.S. POLICY

Anthony H. Cordesman | Center for Strategic & International Studies | August 3, 2020

Over a period of a little more than a month, the U.S. has gone from a mixture of competition and cooperation with China to direct confrontation. This confrontation has also focused largely on the civil level – more specifically on ideology, economics, industrial espionage, cyberattacks on civil networks and databases, and disinformation campaigns. Top Administration officials have given five major speeches which assert that China can no longer be treated as a state evolving towards a more liberal power that will pursue security and economic objectives on terms the U.S. and other states can accept. These speeches assert that China has become an authoritarian state that is driven by a Communist ideology, is seeking to become the world's dominant power, and is using methods of competition that are illegal and violate international norms.

Read the full article here.

CHINA PASSES US AS WORLD'S TOP RESEARCHER, SHOWING ITS R&D MIGHT

NORIAKI KOSHIKAWA | Nikkei Asian Review | August 8, 2020

China has outstripped the U.S. in putting out research papers in the natural sciences, data released Friday shows, further illustrating its emerging dominance in scientific investigation. China now owns the top share of scientific papers at 19.9%, while the U.S. comes in second at 18.3%. These statistics are based on the number of peer-reviewed papers published in scientific journals. This comes as tensions mount between the world's two largest economies on trade and national security. The volume of research being produced by China will have considerable implications for its military and business activities. Between 2016 and 2018, China published an average of 305,927 papers, topping the 281,487 papers released by the U.S. Germany ranks third at 67,041 papers, equating to a 4.4% share.

Read the full article here.

ENHANCED SECURITY REQUIREMENTS FOR PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

Ron Ross, Victoria Pillitteri, Gary Guissanie, Ryan Wagner, Richard Graubart, and Deb Bodeau
National Institute of Standards and Technology | July 2020

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal agencies with recommended enhanced security requirements for protecting the confidentiality of CUI: (1) when the information is resident in nonfederal systems and organizations; (2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI Registry.

Read the full report here.

CHINA IS NOW BLOCKING ALL ENCRYPTED HTTPS TRAFFIC THAT USES TLS 1.3 AND ESNI

Catalin Cimpanu | ZD Net | August 8, 2020

The Chinese government has deployed an update to its national censorship tool, known as the Great Firewall (GFW), to block encrypted HTTPS connections that are being set up using modern, interception-proof protocols and technologies. The ban has been in place for at least a week, since the end of July, according to a joint report published this week by three organizations tracking Chinese censorship -- iYouPort, the University of Maryland, and the Great Firewall Report. Through the new GFW update, Chinese officials are only targeting HTTPS traffic that is being set up with new technologies like TLS 1.3 and ESNI (Encrypted Server Name Indication). Other HTTPS traffic is still allowed through the Great Firewall, if it uses older versions of the same protocols -- such as TLS 1.1 or 1.2, or SNI (Server Name Indication).

Read the full article here.

MANAGING CHAOS: BIOSECURITY IN A POST-COVID-19 AMERICA

Bilva Chandra and Andrew Gonzalez | The Strategy Bridge | August 3, 2020

The ongoing COVID-19 pandemic has asserted new pressures on the United States' national security space due to the exponential nature of biological threats and the lack of a coordinated response. The response has publicly demonstrated the United States' failure to develop and implement a coherent plan, leading the Trump Administration to cease U.S. funding of the World Health Organization, exposing the Administration's tendency for harried decision-making processes. More alarming is how the United States' adversaries seek to exploit similar threats of biological warfare using emerging technologies. These topics are intimately interconnected, and this current crisis elucidates the United States' fragile ability to handle biological threats. Early on in the crisis, the U.S. dithered in implementing stringent travel restrictions and limitations on social interactions to slow the spread of infection and mitigate economic damage simultaneously. Indecisiveness led to the worst of both worlds, in which the infection rate and economic loss outpaced political action. The spread of the coronavirus is not limited to the domestic front.

Read the full article here.

RESEARCHER PLEADED GUILTY TO CONSPIRING TO STEAL SCIENTIFIC TRADE SECRETS FROM OHIO CHILDREN'S HOSPITAL TO SELL IN CHINA

U.S. Department of Justice | July 30, 2020

Former Ohio woman Li Chen, 46, pleaded guilty today via video conference in U.S. District Court today to conspiring to steal scientific trade secrets and conspiring to commit wire fraud concerning the research, identification and treatment of a range of pediatric medical conditions. "Once again we see the People's Republic of China (PRC) facilitating the theft of our nation's ingenuity and hard work as part of their quest to rob, replicate and replace any product they don't have the ability to develop themselves," said John C. Demers, Assistant Attorney General for National Security. "Far from being an isolated incident, we see the PRC implicated in around 60 percent of all trade secret theft cases. This continued economic belligerence runs contrary to the values and norms that facilitate the success of our industries and countering it remains among our highest priorities."

Read the full article here.

REPORT: TWO NEW ENCRYPTION STANDARDS WILL SOON SWEEP AWAY SECURITY CONTROLS

Esther Shein | TechRepublic | August 7, 2020

Transport layer security (TLS) and DNS, two of the foundational protocols of the internet, have recently undergone radical changes to protect browser user privacy. At the same time, they will reduce security on-premises in the short term, and security professionals must put tools in place in the next couple of years, a new report from Forrester Research states. "While [the protocols] hide user activity from the searching eyes of nation-states and ISPs, they also hide valuable metadata from enterprise network inspection tools," according to Forrester Research's senior analyst, David Homes. "As these changes gain momentum, security monitoring tools will be blinded to the contents and destination of traffic and unable to detect threats. The network will be darker than it's ever been."

Read the full article here.

AN ARREST IN CLEVELAND SHOWS HOW CHINA BREAKS THE RULES ON RESEARCH: ROB PORTMAN

Senator Rob Portman | Advance Local Cleveland | August 9, 2020

The coronavirus has challenged our country in unprecedented ways. To overcome this crisis, we are looking in part to our world-class research institutions to help develop treatments and vaccines for this disease. But these places of discovery and innovation are also prime targets for thieves. In May, we were shocked to learn that, in Northeast Ohio, a researcher previously affiliated with the Cleveland Clinic was allegedly stealing research from the Clinic's labs and taking it to China. According to the Department of Justice, this researcher and his research team received more than $3.6 million in U.S. taxpayer-funded grants from the National Institutes of Health (NIH), but hid that he was a dean at a Chinese university. According to the criminal complaint, this researcher, who was also a professor at Case Western Reserve University, received $3 million in funding from the Chinese Communist Party to replicate his Cleveland Clinic research.

Read the full article here.

NEW BILL WOULD BAR IP THEFT OFFENDERS FROM US

Chris Brook | Digital Guardian | August 3, 2020

It's not the first and it certainly won't be the last but on Thursday last week, two U.S. Senators introduced yet another bill designed to crackdown on the theft of U.S. intellectual property. It's the latest in a long line of efforts designed to counter foreign – namely Chinese-backed - IP theft. Two Senators, Chuck Grassley (R-Iowa) and Sheldon Whitehouse (D-R.I.), put forth the latest via legislation - The Stop Theft of Intellectual Property Act (S. 4370) - last week. While previous legislation has sought to heighten awareness of the issue and drill down deeper into how the U.S. handles foreign threats to research, this bill is largely centered around punishing perpetrators of IP theft. The legislation would make foreign nationals deportable and inadmissible if they've violated laws preventing the export of "certain goods, technology or sensitive information, or laws related to economic espionage and the theft or misappropriation of trade secrets."

Read the full article here.

WHY IS THE UNITED STATES EFFECTIVELY BANNING WECHAT AND TIKTOK?

James Palmer | Foreign Policy | August 7, 2020

Following days of speculation, the Trump White House dropped two new executive orders on Thursday night, effectively barring any U.S. transactions with the Chinese social media apps TikTok and WeChat. The decision was made under the authority of the International Emergency Economic Powers Act that underlies U.S. sanctions programs. Amid a flurry of actions directed against China by the administration in recent weeks, including the rollout of a wide-ranging but unclear Clean Network program, this is perhaps the most significant. The new restrictions on the popular video-sharing app TikTok increase the likelihood of a quick sale to Microsoft, the U.S. software giant that has expressed interest in a purchase. It would likely be easy to slice off TikTok from its original Chinese ownership since it was set up as a separate system in the first place. WeChat, by contrast, is the same app in the United States as it is in China.

Read the full article here.

UNIVERSITY OF ARKANSAS PROFESSOR INDICTED FOR WIRE FRAUD AND PASSPORT FRAUD

U.S. Department of Justice | July 29, 2020

The Department of Justice announced today that Simon Saw-Teong Ang, 63, of Fayetteville, Arkansas, was indicted by a federal grand jury in the Western District of Arkansas on 42 counts of wire fraud and two counts of passport fraud. "Transparency and integrity have long sustained the pursuit of knowledge on America's campuses," said Assistant Attorney General for National Security John C. Demers. "Mr. Ang is alleged to have demonstrated neither when he failed to disclose his financial and other ties to companies and institutions in China to the University of Arkansas and to U.S. government agencies, despite an obligation to do so. This is a hallmark of the China's targeting of research and academic collaborations within the United States in order to obtain U.S. technology illegally. The Department of Justice will continue to work with colleges and universities to protect U.S. research and development from exploitation by foreign powers and will prosecute those who defraud the U.S. Government."

Read the full article here.

PROTECTING KEY ASSETS: A CORPORATE COUNTERINTELLIGENCE GUIDE

U.S. Office of the National Counterintelligence Executive

"A disturbing trend has developed in which foreign intelligence services, non-state actors, and criminals are using intelligence collection techniques against American companies to steal valuable trade secrets and assets. This activity can bankrupt a company by compromising years of costly research and development, weaken the U.S. economy, and threaten national security. According to the FBI, the cost to U.S. industry is tens of billions of dollars each year. Corporate boards and executive officers must understand the true threat their companies face. It is one that has evolved beyond the stage where information security, as one example, can simply be delegated to the security office or CIO [chief information officer] - it requires full executive engagement. With the tools available to economic spies, the American private sector is more vulnerable than ever."

Read the full guide here.

CHINESE WHISPERS CENSORED: HOW CHINA'S COMMUNIST PARTY HAS LENS ON DISSENT BY OVERSEAS STUDENTS

Saikiran Kannan | India Today | August 7, 2020

The Chinese Communist Party (CCP) in an attempt to control the opinion of China's overseas students has started an online portal that allows Chinese citizens to identify and call out their own for 'political crimes', sparking fears of censorship among the international students and academics. The portal can be accessed by Chinese citizens across the world. This has come to light after the recent controversy in Australia's University of New South Wales (UNSW) over an article published on its website raising concerns about human rights in China and other regions like Hong Kong under its control. An aggressive online campaign was launched targeting the university and rallying support of Chinese students. China's handling of Hong Kong and the introduction of the National Security Law were heavily scrutinized and covered internationally. It was a chance for the world to see how China handles democratic dissent and political activism.

Read the full article here.

NOT JUST SEEDS—ALL KINDS OF MYSTERY PACKAGES ARE ARRIVING FROM CHINA

Seren Morris | Newsweek | August 5, 2020

I t's not just seeds—Americans are receiving all kinds of unsolicited packages from China, containing items ranging from fake Ray-Ban sunglasses to a pair of used socks. The United States Department of Agriculture believes that the mystery seeds were being sent to the U.S. as part of a brushing scam, which involves sellers sending unsolicited items (which are typically light and easy to ship) and then post fake customer reviews to boost sales. The USDA said in a statement: "At this time, we don't have any evidence indicating this is something other than a 'brushing scam' where people receive unsolicited items from a seller who then posts false customer reviews to boost sales.

Read the full article here.

US GOVT EXPOSES CHINESE ESPIONAGE MALWARE SECRETLY USED SINCE 2008

Sergiu Gatlan | Bleeping Computer | August 3, 2020

The U.S. government today released information on a malware variant used by Chinese government-sponsored hackers in cyber espionage campaigns targeting governments, corporations, and think tanks. The new malware is a remote access trojan (RAT) dubbed TAIDOOR actively used by Chinese government cyber actors according to information published today by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Defense (DoD). "China's Taidoor malware has been compromising systems since 2008," U.S. Cyber Command also tweeted today. U.S. Cyber Command has also uploaded four samples of the newly discovered RAT malware variants onto the VirusTotal malware aggregation repository.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu