RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

February 29, 2024

U.S. STATE GOVERNMENT NETWORK BREACHED VIA FORMER EMPLOYEE'S ACCOUNT

The Hacker News | February 16, 2024

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has revealed that an unnamed state government organization's network environment was compromised via an administrator account belonging to a former employee. "This allowed the threat actor to successfully authenticate to an internal virtual private network (VPN) access point," the agency said in a joint advisory published Thursday alongside the Multi-State Information Sharing and Analysis Center (MS-ISAC). "The threat actor connected to the [virtual machine] through the victim's VPN with the intent to blend in with legitimate traffic to evade detection." It's suspected that the threat actor obtained the credentials following a separate data breach owing to the fact that the credentials appeared in publicly available channels containing leaked account information. The admin account, which had access to a virtualized SharePoint server, also enabled the attackers to access another set of credentials stored in the server, which had administrative privileges to both the on-premises network and the Azure Active Directory (now called Microsoft Entra ID).

Read the full article here.

U.S. DEFENSE REQUIRES GREATER CIVIL SUPPORT TO COUNTER CHINA'S CYBER AGGRESSION

Bob Kolasky | Defense Opinion | February 7, 2024

While much of Washington was transfixed recently by Meta CEO Mark Zuckerberg apologizing at a Senate hearing to families who had lost loved ones to online harassment, the national security community's attention was focused on another Capitol Hill gathering related to digital malfeasance. The country's four top cybersecurity officials—the newly appointed National Cyber Director and the heads of U.S. Cyber Command, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA)—delivered a dramatic message to a House panel: the country's critical infrastructure is under cyberattack from the Chinese government. FBI Director Christopher Wray said that the Chinese Communist Party's (CCP) multi-pronged assault on the U.S. economic and national security was the defining threat of a generation. What was especially interesting about the hearing to cybersecurity professionals was not that the message was new. The U.S. government has long experienced foreign governments, including the Chinese government, attempting to (and sometimes successfully) breach critical infrastructure systems. In 2018, for example, the then-Director of National Intelligence, Dan Coats, said: "The warning lights are blinking red on cyber attacks."

Read the full article here.

MICROSOFT AZURE HIT WITH THE LARGEST DATA BREACH IN ITS HISTORY; HUNDREDS OF EXECUTIVE ACCOUNTS COMPROMISED

Krishi Chowdhary | TechReport | February 21, 2024

For the first time in the history of Microsoft, a cyberattack has left hundreds of executive accounts compromised and caused a major user data leak as Microsoft Azure was attacked. According to Proofpoint, the hackers use the malicious techniques that were discovered in November 2023. It includes credential theft through phishing methods and cloud account takeover (CTO) which helped the hackers gain access to both Microsoft365 applications as well as OfficeHome. The reason why so many people fell for this attack was because it was carried out through malicious links embedded in documents. These links led to phishing websites but the anchor text of these links was "View Document". Naturally, no one was suspicious of a text like that.

Read the full article here.

WHERE FREEDOM MEETS REPRESSION: AUSTRALIAN ACADEMICS TREAD A FINE LINE OVER TIES TO IRAN

Jonathan Yerushalmy | The Guardian | February 24, 2024

In April 2023 the Iranian government was in the midst of a brutal crackdown. Weeks earlier, thousands had been on the streets, protesting against the death in custody of Mahsa Amini, a 22-year-old detained for an alleged violation of the country's strict dress codes for women. That month, with hundreds of Iranians who had taken part in the demonstrations dead or in jail, and the regime ramping up its repressive tactics, the Australian foreign minister wrote to more than 30 university vice-chancellors and presidents. In the letter, Penny Wong outlined the government's concern over the human rights situation in Iran and asked the university leaders to pause joint work with Iranian institutions. "I urge you to join with the Government to put on hold existing cooperation with Iranian entities, including … universities, and to refrain from any proposed new engagement," Wong wrote.

Read the full article here.

CENSORSHIP PRACTICES OF THE PEOPLE'S REPUBLIC OF CHINA

The U.S.-China Economic and Security Review Commission | February 20, 2024

This report, prepared for the Commission by Exovera's Center for Intelligence Research and Analysis (CIRA), examines the elaborate and pervasive censorship apparatus used by the People's Republic of China (PRC) and the Chinese Communist Party (CCP) to maintain the Party's monopoly on political legitimacy, shape the behavior of China's citizenry, and control information beyond its borders.

Some Key Findings Include:

- Under General Secretary of the CCP Xi Jinping's rule, the Party has significantly expanded the scope and stringency of its censorship apparatus, with a particular focus on solidifying its control over internet content. At the same time, the CCP allows for limited discussions of sensitive topics that do not directly threaten its hold on power, such as China's role in the ongoing Russia-Ukraine conflict.
- Despite the importance the CCP places on domestic information control, its censorship apparatus is unevenly developed and plagued by unfunded mandates. The PRC's policy of assigning legal liability to internet service providers (ISPs) and private website owners has driven these entities to self-police and censor content posted on their platforms.

Read the full article here.

EMERGING MILITARY TECHNOLOGIES: BACKGROUND AND ISSUES FOR CONGRESS

Kelley M. Sayler | Congressional Research Service | February 22, 2024

Members of Congress and Pentagon officials are increasingly focused on developing emerging military technologies to enhance U.S. national security and keep pace with U.S. competitors. The U.S. military has long relied upon technological superiority to ensure its dominance in conflict and to underwrite U.S. national security. In recent years, however, technology has both rapidly evolved and rapidly proliferated—largely as a result of advances in the commercial sector. As former Secretary of Defense Chuck Hagel observed, this development has threatened to erode the United States' traditional sources of military advantage. The Department of Defense (DOD) has undertaken a number of initiatives to arrest this trend. For example, in 2014, DOD announced the Third Offset Strategy, an effort to exploit emerging technologies for military and security purposes as well as associated strategies, tactics, and concepts of operation. In support of this strategy, DOD established a number of organizations focused on defense innovation, including the Defense Innovation Unit and the Defense Wargaming Alignment Group.

Read the full article here.

GERMAN SCIENCE MINISTER CALLS FOR A RETHINK OF "STRONG WALL" BETWEEN CIVILIAN AND MILITARY RESEARCH

David Matthews | Science Business | February 20, 2024

At the Munich Security Conference, Bettina Stark-Watzinger made the case that research is now at the centre of geopolitical rivalry. But changing the German research system remains difficult. Germany's science minister has called for a rethink of the country's traditional separation between civilian and military research during an unprecedented debate on research security at the Munich Security Conference. More normally the haunt of generals than science ministers, Bettina Stark-Watzinger's appearance at the conference is a mark of how dramatically security concerns, particularly around China, are now part of science and innovation policy. "It is a strong signal, that research is a geopolitical factor," said Stark-Watzinger during a panel debate on 16 February. Back in 2016, the then EU research Commissioner Carlos Moedas was trumpeting the EU's Horizon 2020 research programme as "open to the world."

Read the full article here.

THE CHINA-US QUANTUM RACE

Sam Howell | The Diplomat | January 13, 2023

Quantum researchers in China claim to have an algorithm capable of breaking public-key encryption, years before anyone expected. Accurate or not, the announcement serves as a reminder that surprising quantum breakthroughs are possible in the near term. If the Biden administration is serious about its designation of quantum information science (QIS) as a critical technology area for national security, it must do more to safeguard U.S. quantum superiority. QIS uses the laws of quantum physics, which describes the properties of nature on a tiny scale, to advance the processing, analysis, and transmission of information. Quantum computing, quantum encryption, and quantum sensing constitute the three primary domains within QIS. Although it is an evolving field, QIS promises to transform almost any industry dependent on speed and processing power, from aerospace and automotive to finance and pharmaceuticals.

Read the full article here.

INDIA, THE US LOOKING INTO EXCITING JOINT SCIENCE & TECHNOLOGY PROJECTS TO FURTHER EXPAND TIES: TOP AMERICAN SCIENTIST

Financial Express | February 21, 2024

India and the US are looking into exciting joint science and technology projects to further expand their relationship under the guidance of the top leadership of the two countries, according to a top American scientist. Describing the US-India Partnership as a very important one for the Biden-Harris administration and also in Congress, Dr Sethuraman Panchanathan, Director of the National Science Foundation said there's total bipartisan support for a strong partnership between two great democracies, the US and India. Last year, Prime Minister Narendra Modi kicked off his visit to Washington DC, for the historic State Visit, with a trip to the National Science Foundation headquarters in Alexandria wherein he interacted with the scientific community and the young scientist minds. "Now, in terms of the National Science Foundation (NSF), we have started to work with India in the science and technology front with threads of partnerships, as I call them," Panchanathan told PTI in an interview.

Read the full article here.

FIXING THE NATION'S CLASSIFICATION SYSTEM

Heather McMahon | The Washington Post | February 20, 2024

The Feb. 14 editorial, "The secret about America's secrets," addressed the government's overclassification problem in light of President Biden's and former president Donald Trump's mishandling of classified materials. The editorial noted that not only is there a problem with overclassification but also the process itself is overly complex, with more than 2,000 classification guides. As a former intelligence officer, I not only agree that the system should be simplified but also believe classified information shouldn't be printed on paper in the first place. Boxes of classified documents were stored at Mr. Biden's and Mr. Trump's homes because the government has not been able to end its relationship with paper. The good news is that that's changing. In June, a federal mandate goes into effect requiring all documents to be stored digitally. This is a huge initiative that will ultimately make it easier to manage and protect classified information while improving government transparency.

Read the full article here.

IOS, ANDROID MALWARE STEALS FACES TO DEFEAT BIOMETRICS WITH AI SWAPS

Nate Nelson | DarkReading | February 15, 2024

Southeast Asia is learning the hard way that biometric scans are nearly as easy to bypass as other kinds of authentication data, thanks to a creative banking Trojan. Chinese hackers have developed a sophisticated banking Trojan for tricking people into giving up their personal IDs, phone numbers, and face scans, which they're then using to log into those victims' bank accounts. The new malware, "GoldPickaxe," was developed by a large (but unidentified) Chinese-language group. Its variants work across iOS and Android devices, masquerading as a government service app in order to trick primarily elderly victims into scanning their faces. The attackers then use those scans to develop deepfakes that can bypass cutting-edge biometric security checks at Southeast Asian banks. In a new report, researchers from Group-IB identified at least one individual whom they believe to be an early victim: a Vietnamese citizen, who earlier this month lost around $40,000 dollars as a result of the ruse.

Read the full article here.

US RIVALRY WITH CHINA EXPANDS TO BIOTECH. LAWMAKERS SEE A FAILURE TO COMPETE AND WANT TO ACT

Didi Tang | Associated Press News | February 18, 2024

U.S. lawmakers are raising alarms about what they see as America's failure to compete with China in biotechnology, warning of the risks to U.S. national security and commercial interests. But as the two countries' rivalry expands into the biotech industry, some say that shutting out Chinese companies would only hurt the U.S. Biotechnology promises to revolutionize everyday life, with scientists and researchers using it to make rapid advances in medical treatment, genetic engineering in agriculture and novel biomaterials. Because of its potential, it has caught the attention of both the Chinese and U.S. governments. Bills have been introduced in the House and Senate to bar "foreign adversary biotech companies of concern" from doing business with federally funded medical providers. The bills name four Chinese-owned companies.

Read the full article here.

WHY FAKE RESEARCH IS RAMPANT IN CHINA

The Economist | February 22, 2024

Huang Feiruo was once a respected scientist who studied ways to make pigs gain weight more quickly. He ran government-funded research projects at Huazhong Agricultural University in the central city of Wuhan. But last month 11 of his graduate students accused him of plagiarising the work of other academics and fabricating data. He had also, they said, put pressure on them to fake their own research. On February 6th the university announced that it had fired Mr. Huang and retracted some of his work. Scientific fraud is all too common in China. Bad incentives are a big part of the problem. Chinese universities typically reward researchers with promotions and funding based on the quantity of papers they publish, not the quality. That has got results. In 2017, for the first time, China published more scientific papers than any other country. It has kept the top spot ever since. But while some of the research has been cutting-edge, much has been dodgy.

Read the full article here.

WANTED: SCIENTIFIC ERRORS. CASH REWARD.

Stephanie M. Lee | The Chronicle of Higher Education | February 12, 2024

Scientific-misconduct accusations are leading to retractions of high-profile papers, forcing reckonings within fields and ending professorships, even presidencies. But there's no telling how widespread errors are in research: As it is, they're largely brought to light by unpaid volunteers. A program launching this month is hoping to shake up that incentive structure. Backed by 250,000 Swiss francs, or roughly $285,000, in funding from the University of Bern, in Switzerland, it will pay reviewers to root out mistakes in influential papers, beginning with a handful in psychology. The more errors found, and the more severe they are, the more the sleuths stand to make. The tech industry has long paid bounty hunters to unearth bugs in code, but the scientific enterprise has not had an equivalent — to its detriment, many say.

Read the full article here.

USEFUL RESOURCES

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROPOSED RULE OVERVIEW

U.S. Department of Defense | February 7, 2024

The video above provides an overview of the Cybersecurity Maturity Model Certification (CMMC) Program 32 Code of Federal Regulations (CFR) proposed rule, which was published in the Federal Register for public comment on December 26, 2023. Electronic comment submissions on the proposed rule and supplemental documents should be filed online at the following Regulations.gov webpages prior to the close of the public comment period on February 26, 2024.

Read the full article here.

U.S. BUSINESS RISK: PEOPLE'S REPUBLIC OF CHINA (PRC) LAWS EXPAND BEIJING'S OVERSIGHT OF FOREIGN AND DOMESTIC COMPANIES

The National Counterintelligence and Security Center | Safeguarding our Future | June 20, 2023

Since 2015, the PRC has passed or updated comprehensive national security, cybersecurity, and data privacy laws and regulations, expanding Beijing's oversight of domestic and foreign (including U.S.) companies operating within China. Beijing views inadequate government control of information within China and its outbound flow as a national security risk. These laws provide the PRC government with expanded legal grounds for accessing and controlling data held by U.S. firms in China. U.S. companies and individuals in China could also face penalties for traditional business activities that Beijing deems acts of espionage or for actions that Beijing believes assist foreign sanctions against China.

Read the full article here.

CYBERSECURITY RESOURCES FOR HIPAA-REGULATED ENTITIES

National Institute of Standards and Technology | February 14, 2024

This is a listing of resources (e.g., guidance, templates, tools) that regulated entities may find useful for achieving compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and improving the security posture of their organizations. This list of resources complements guidance provided to regulated entities in Special Publication (SP) 800-66r2.

Read the full article here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute