ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM
https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

August 17, 2023

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

August 2023

NCSC executes the roles and responsibilities of the National Operations Security (OPSEC) Program Office, as described in National Security Presidential Memorandum (NSPM)-28 and will support department and agency implementation of OPSEC programs. NCSC/ETD will provide additional guidance, work with all Executive Branch departments and agencies to develop their programs, and will provide program development, training, and awareness materials. As set forth in NSPM-28, the National Operations Security Program (NOP) supports the establishment, implementation, and standardization of stakeholder OPSEC programs across the Executive Branch of the U.S. Government (USG) and, as appropriate, beyond to trusted partners. NSPM-28 requires all Executive Branch departments and agencies to implement OPSEC capabilities that identify and protect their most critical assets, identify and mitigate vulnerabilities, consider foreign adversarial threats in their organization's risk management activities, and apply sufficient threat mitigation practices to counter the threat. NOP requirements are set forth in NSPM-28.

Read the full article here.

CHINESE THREAT GROUP APT41 LINKED TO ANDROID MALWARE ATTACKS

Jayant Chakravarti | GovInfoSecurity | July 20, 2023

Security researchers say a Chinese state-sponsored espionage group is using WyrmSpy and DragonEgg surveillance malware to target Android mobile devices. Researchers at cybersecurity company Lookout said APT41, also tracked as Barium, Earth Baku and Winnti, primarily relies on web application attacks and software vulnerabilities and uses WyrmSpy and DragonEgg to target organizations globally. The company said APT41 recently switched tactics to develop malware specific to the Android operating system, relying on existing command-and-control infrastructure, IP addresses and domains to communicate with and issue commands to the two malware variants. APT41 historically exploited specific web applications and software vulnerabilities to carry out surveillance on predefined target organizations. According to Mandiant, the group in May 2021 exploited a zero-day vulnerability in the USAHerds application and several vulnerable internet-facing web applications to successfully compromise at least six U.S. state government networks.

Read the full article here.

CHINA SCHOLARSHIP COUNCIL AND UNIVERSITY OF MELBOURNE PARTNERSHIP TO FUND PHD CANDIDATES UNTIL 2027

The University of Melbourne | July 5, 2023

The University of Melbourne today announced a partnership renewal with the China Scholarship Council for a combined investment of up to AUD$75 million. Under this partnership, the China Scholarship Council and the University co-fund scholarships for top-ranking graduates from institutions in China wishing to undertake a Doctor of Philosophy (PhD) at the University of Melbourne and will support up to 180 candidates over the next four years. University of Melbourne Vice-Chancellor Professor Duncan Maskell announced the agreement renewal while leading a University delegation in China. Professor Maskell said the scholarships are an important part of the University's commitment to supporting international education and research. "We value our strong and longstanding partnership with the China Scholarship Council, which is vital in fostering global research and knowledge sharing," Professor Maskell said. "As a university, we recognise the important role we play to support opportunities for global education.

Read the full article here.

TO BATTLE NEW THREATS, SPY AGENCIES TO SHARE MORE INTELLIGENCE WITH PRIVATE SECTOR

Warren P. Strobel | The Wall Street Journal | August 10, 2023

U.S. spy agencies will share more intelligence with U.S. companies, nongovernmental organizations and academia under a new strategy released this week that acknowledges concerns over new threats, such as another pandemic and increasing cyberattacks. The National Intelligence Strategy, which sets broad goals for the sprawling U.S. intelligence community, says that spy agencies must reach beyond the traditional walls of secrecy and partner with outside groups to detect and deter supply-chain disruptions, infectious diseases and other growing transnational threats. The intelligence community "must rethink its approach to exchanging information and insights," the strategy says. The U.S. government in recent years has begun sharing vast amounts of cyber-threat intelligence with U.S. companies, utilities and others who are often the main targets of foreign hackers, as well as information on foreign-influence operations with social-media companies.

Read the full article here.

AFTER A RECENT HACKING—WHAT ARE THE RISKS AND REWARDS OF CLOUD COMPUTING USE BY THE FEDERAL GOVERNMENT?

U.S. Government Accountability Office | August 10, 2023

Cloud computing offers significant opportunities to increase government efficiency, as well as customer service-like benefits for the public. The federal government has recognized these benefits and is increasingly using cloud computing services for things like access to shared resources such as networks, servers, and data storage. But without effective security measures, these services can also make federal agencies and their computer systems vulnerable to cyberattack. This vulnerability was reported in July, after the State Department and other agencies had their cloud-based emails hacked by Chinese-based threat actors. What should the federal government do to better secure their cloud computing services from attacks like these and what are the risks to taxpayers? Today's WatchBlog post looks at our recent report and other work.

Read the full article here.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER POST

August 9, 2023

Director of National Intelligence Avril Haines debuts the 2023 National Intelligence Strategy today, mapping out the most critical challenges and pivotal opportunities facing the U.S. Intelligence Community and our rapidly evolving world over the next four years. "The National Intelligence Strategy articulates what the Intelligence Community will need to cultivate to be effective in the future: an information and technological edge, a broad array of partnerships, and a talented and diverse workforce as we pursue our vision of an IC that embodies America's values," shared DNI Haines. Our next four years are marked by strategic competition among the U.S., China, and Russia; the surging importance of emerging technologies, supply chains, and economics to national security; the increasing influence of sub-national and non-state actors; and issues triggered by the convergence of shared global challenges, like climate change and health security.

Read the full article here.

NSA CHIEF: CHINESE CYBER SPIES CONTINUE TO IMPROVE — BUT HAVEN'T SURPASSED US

Martin Matishak | The Record | August 10, 2023

China has not yet surpassed the U.S. in conducting cyber espionage despite several successful hacks that have been publicly linked to Beijing, the head of the U.S.'s premier digital spy agency said Thursday. "No. No. No," Army Gen. Paul Nakasone, the outgoing director of the National Security Agency and the head of U.S. Cyber Command, answered during a discussion at the Center for Strategic and International Studies in Washington when asked if the U.S. had been eclipsed. But, he added, the skills used by Chinese hackers and the scope of their online attacks continues to improve. "Are they getting better? Yes." The comments come after a series of reports that China, which spent years pilfering American intellectual property, was responsible for a number of sophisticated hacks, such as breaking into the emails of a group of senior U.S. officials like Commerce Secretary Gina Raimondo and the country's ambassador to China.

Read the full article here.

A NEW WHITE HOUSE ORDER IS TAKING AIM AT INVESTMENT IN CHINESE TECH. HOW WILL IT ACTUALLY WORK?

Sarah Bauerle Danzman and Emily Weinstein | Atlantic Council | August 10, 2023

The Biden administration has put forward plans to require certain US persons to notify the US government in advance of making certain types of investment in People's Republic of China (PRC) entities. In particular, the United States is interested in entities engaged in activities related to "covered national security technology or products." The White House released a long-anticipated Executive Order on August 9 that directs the Treasury Department, in consultation with the Commerce Department, to develop a new regulatory system for these notifications. This may at first sound narrow and procedural, but it has important implications for US national security and US-China trade. In addition, the new regulations will prohibit US persons from engaging in certain investment transactions with covered foreign parties. The order gives the Treasury Department the authority to, in conjunction with the interagency, identify the types of transactions and technologies that may pose a risk to US national security and thereby warrant notification or prohibition.

Read the full article here.

CHINA-LINKED HACKERS STRIKE WORLDWIDE: 17 NATIONS HIT IN 3-YEAR CYBER CAMPAIGN

The Hacker News | August 9, 2023

Hackers associated with China's Ministry of State Security (MSS) have been linked to attacks in 17 different countries in Asia, Europe, and North America from 2021 to 2023. Cybersecurity firm Recorded Future attributed the intrusion set to a nation-state group it tracks under the name RedHotel (previously Threat Activity Group-22 or TAG-22), which overlaps with a cluster of activity broadly monitored as Aquatic Panda, Bronze University, Charcoal Typhoon, Earth Lusca, and Red Scylla (or Red Dev 10). Active since 2019, some of the prominent sectors targeted by the prolific actor encompass academia, aerospace, government, media, telecommunications, and research. A majority of the victims during the period were government organizations. "RedHotel has a dual mission of intelligence gathering and economic espionage," the cybersecurity company said, calling out its persistence, operational intensity, and global reach.

Read the full article here.

U.S. RAISES CONCERNS OVER CHINA'S COUNTER-ESPIONAGE PUSH

By Daphne Psaledakis and Humeyra Pamuk | Reuters | August 2, 2023

The United States on Wednesday raised concerns over a Chinese call to encourage its citizens to join counter-espionage work and said it has been closely monitoring the implementation of Beijing's expanded anti-spying law. China's Ministry of State Security on Tuesday said China should encourage its citizens to join counter-espionage work, including creating channels for individuals to report suspicious activity and rewarding them for doing do. A system that makes it "normal" for regular people to participate in counter-espionage should be established, the ministry said. That followed an expansion of China's counter-espionage law that took effect in July and bans the transfer of information it sees as related to national security. It has alarmed the United States, which has warned that foreign companies in China could be punished for regular business activities. "We do have concerns over it, certainly encouraging citizens to spy on each other is something that's of great concern," State Department spokesperson Matt Miller told a daily news briefing.

Read the full article here.

SPUTTERING ECONOMY + FLOODS AROUND BEIJING + END OF ITALY'S BRI PACT

MERICS | August 10, 2023

China's post-Covid economic recovery, once expected to be strong as the country emerged from lockdowns in 2022, seems to have foundered. Consumers and business leaders are struggling with mixed signals from policy makers. Trade data this week revealed exports were down 14 percent year-on-year, their largest decline since February 2020, while imports fell 12.4 percent, far more steeply than expected. These developments, the most recent in a series of lackluster economic data, have undermined expectations for a robust recovery and are suppressing confidence among policy makers and investors. The Chinese government has tried to soothe markets with a haphazard flurry of assurances and policy measures. Last month, the Chinese Communist Party’s (CCP’s) Central Committee and the State Council issued a 31-point action plan to make the private sector “bigger, better and stronger” – language usually applied to state-owned enterprises under President Xi Jinping’s governance.

Read the full article here.

HOW TO REMOVE YOUR INFO FROM GOOGLE WITH THE 'RESULTS ABOUT YOU' TOOL

Reece Rogers | Publication | August 9, 2023

In 2022, GOOGLE launched the “Results about you” tool to help people remove personal info from the company’s search results. With billions of searches happening daily on Google, finding your private phone number or home address indexed for the world to see can be quite shocking. Luckily, new updates to “Results about you” make it easier to discover when your data pops up in Search. Previously, you had to proactively find the links of sites hosting your personal data to report and request the removal of identifiable information. Now, you’ll be able to set up alerts for whenever your email, home address, or phone number appear on Google. At first, this update will only be available in the US and scan for results just in English. “Results about you” is accessible in your browser or through the mobile app. For browsers, log into Google or create an account, then visit this webpage to get started.

Read the full article here.

WITH AI, HACKERS CAN SIMPLY TALK COMPUTERS INTO MISBEHAVING

Robert McMillian | The Wall Street Journal | August 10, 2023

ChatGPT’s ability to respond quickly and effectively to simple commands has attracted more than 100 million users, and a few hackers along the way. Johann Rehberger, a security researcher, is one of them. Using plain English, he recently coaxed OpenAI’s chatbot to do something bad: Read his email, summarize it and post that information to the internet. In the hands of a criminal, this technique could have been used to steal sensitive data from someone’s email inbox, Rehberger said. ChatGPT “lowers the barrier to entry for all sorts of attacks,” Rehberger said. “Because you don’t really need to be able to write code. You don’t have to have that deep knowledge of computer science or hacking.” The attack wouldn’t have affected most ChatGPT accounts. It worked because Rehberger was using a beta-test feature of ChatGPT that gave it access to apps such as Slack, Gmail and others.

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