ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

December 21, 2022

NSA SAYS CHINESE HACKERS ARE ACTIVELY ATTACKING FLAW IN WIDELY USED NETWORKING DEVICE

Elias Groll | CyberScoop | December 13, 2022

The National Security Agency said on Tuesday that Chinese state-backed hackers are exploiting a flaw in a widely used networking device that allows an attacker to carry out remote code execution. In its advisory, the NSA said it believes a Chinese hacking crew known as APT5 "has demonstrated capabilities" against an application delivery controller made by Citrix. Citrix released an emergency patch to fix the vulnerability on Monday and said that "exploits of this issue on unmitigated appliances in the wild have been reported." The spy agency's advisory effectively burns down an apparent Chinese intelligence operation by exposing its tools and advising potential victims on how to prevent further attacks. The NSA has historically preferred to monitor such attacks rather than publicizing them, but in recent years it has grown more proactive in sharing intelligence on attackers such as APT5. Now that they've been burned, the hackers behind the operation targeting Citrix may step up the pace of their attacks.

Read the full article here.

GUIDANCE ON SCIENTIFIC AND TECHNOLOGICAL COOPERATION WITH THE RUSSIAN FEDERATION FOR U.S. GOVERNMENT AND U.S. GOVERNMENT AFFILIATED ORGANIZATIONS

The White House | June 11, 2022

The United States is committed to international scientific cooperation that flows from the mutual recognition of shared values, including scientific freedom, openness, transparency, honesty, equity, fair competition, objectivity, and democratic principles. The Kremlin's unlawful and unprovoked full-scale invasion of Ukraine is an affront to the principles we seek to affirm and our efforts to advance international science, technology, and innovation for development. We remain concerned that the Kremlin continues to leverage state-controlled institutions to aid in its disinformation campaign against Ukraine. In response to Putin's aggression, the U.S. government has taken active measures to limit bilateral science and technology research cooperation with the Russian government. Consistent with U.S. domestic and international law, we will wind down institutional, administrative, funding, and personnel relationships and research collaborations in the fields of science and technology with Russian government-affiliated research institutions and individuals who continue to be employed by or work under the direction of those institutions.

Read the full article here.

PEOPLE'S REPUBLIC OF CHINA CITIZEN ARRESTED FOR STALKING

U.S. Attorney's Office, District of Massachusetts | U.S. Department of Justice | December 14, 2022

A Berklee College of Music student, who is citizen of the People's Republic of China (PRC), has been arrested and charged with stalking in connection with threatening and harassing communications he allegedly made towards an individual who posted fliers in support of democracy in China. Xiaolei Wu, 25, was charged with one count of stalking and will make an initial appearance in federal court in Boston this afternoon. Wu has lived in Boston while attending the Berklee College of Music. Wu will appear in federal court in Boston at 3 p.m. this afternoon. According to the charging documents, on Oct. 22, 2022, an individual posted a flier on or near the Berklee College of Music campus in Boston which said, "Stand with Chinese People," as well as, "We Want Freedom," and "We Want Democracy." It is alleged that, beginning on or about Oct. 22, 2022 and continuing until Oct. 24, 2022, Wu made a series of communications via WeChat, email and Instagram directed towards the victim who posted the flier.

Read the full article here.

STOLEN DATA ON 80K+ MEMBERS OF FBI-RUN INFRAGARD REPORTEDLY FOR SALE ON DARK WEB FORUM

Jai Vijayan | Dark Reading | December 15, 2022

A hacker using the handle "USDoD" has reportedly stolen contact information on more than 80,000 members of an FBI-run program called InfraGard and put the information up for sale on an English-speaking Dark Web forum. The information the hacker accessed from InfraGard's database appears to be fairly basic and in some cases does not even include an email address, according to KrebsOnSecurity, which first reported on the incident this week. But the information belongs to CISOs, security directors, IT and C-suite executives, healthcare professionals, emergency managers, and law enforcement and military personnel directly responsible for protecting US critical infrastructure. As such, the stolen data represents a valuable asset for adversaries, says former InfraGard member Chris Pierson, currently CEO of BlackCloak, an online privacy-protection service for top executives and corporate leaders. "The InfraGard database of contacts is a big win for any intelligence agency or nation-state to possess," Pierson says. The compromised data is nowhere close in sensitivity compared to major breaches such as the one that the US Office of Personnel Management (OPM) disclosed in 2015. Still, it is very practical and easy to use from an attacker's perspective, he says.

Read the full article here.

PERSONNEL OF THE PEOPLE'S LIBERATION ARMY

Kenneth W. Allen, Thomas Corbett, Taylor A. Lee, and Ma Xiu | U.S.-China Economic and Security | BluePath Labs | November 3, 2022

This report conducts an in-depth assessment of various personnel-related topics in the People's Liberation Army (PLA), as requested by the U.S.-China Economic and Security Review Commission (USCC). Information is drawn primarily from open-source research and analysis of Chinese documents, regulations, newspaper articles, and books, as well as from authoritative secondary sources. Topics include PLA personnel quality and shortfalls, challenges the PLA faces in improving personnel quality, recruiting and retention of quality personnel, desired education and expertise, conscription vs. voluntary recruitment, morale, combat readiness, personnel socioeconomic makeup, and the role of politics in the PLA. Among the key findings, this report suggests that Xi Jinping has continued doubts about personnel competence and loyalty since becoming the Chairman of the Central Military Commission in 2012, and thus has focused on both force modernization and Party loyalty.

Read the full article here.

RUSSIAN SECRET SERVICE TO VET RESEARCH PAPERS

Quirin Schiermeier | Nature | October 20, 2015

A biology institute at Russia's largest and most prestigious university has instructed its scientists to get all research manuscripts approved by the security service before submitting them to conferences or journals. The instructions, which come in response to an amended law on state secrets, appear in minutes from a meeting held on 5 October at the A. N. Belozersky Institute of Physico-Chemical Biology at Lomonosov Moscow State University (MSU). The Russian government says that the amendment is not designed to restrict the publication of basic, non-military research. But scientists say that they believe institutes across the country are issuing similar orders. "This is a return to Soviet times when in order to send a paper to an international journal, we had to get a permission specifying that the result is not new and important and hence may be published abroad," says Mikhail Gelfand, a bioinformatician at MSU. In 1993, the government passed a law obliging scientists in Russia to get permission from the Federal Security Service (FSB) before publishing results that might have military or industrial significance. This mainly covered work that related to building weapons, including nuclear, biological and chemical ones.

Read the full article here.

CLARIVATE, THE CHINESE ACADEMY OF ENGINEERING AND THE HIGHER EDUCATION PRESS OF CHINA RELEASE ANNUAL JOINT REPORT TO IDENTIFY 188 ENGINEERING FRONTS

Clarivate | December 15, 2022

Clarivate Plc (NYSE: CLVT), a global leader in providing trusted information and insights to accelerate the pace of innovation, the Chinese Academy of Engineering (CAE), and the Higher Education Press of China today released their sixth annual collaborative report – Engineering Fronts 2022. The report, which was launched at a joint forum in Beijing, has identified 188 of the most important areas in engineering research and development. In the report, an engineering front is defined as a key direction which is forward looking, leading and exploratory. It has a major influence, plays a leading role in the future of engineering science and technology and serves as an important guide for cultivating innovation. The Engineering research fronts focus on theoretical exploration and are identified using citation data from Clarivate's Web of Science™ as well as nominations by experts in China's engineering research institutions.

Read the full article here.

U.S. WIDENS BAN ON MILITARY AND SURVEILLANCE TECH SALES TO CHINA

Ellen Nakashima, Jeanne Whalen, and Cate Cadell | The Washington Post | December 15, 2022

The Biden administration doubled down Thursday on its high-tech containment of China, expanding a ban on commercial exports of advanced U.S. technology that it said aids Beijing's military and hypersonics programs and enables human rights violations. The addition of some three dozen Chinese companies to a U.S. export blacklist, including one of the country's largest chipmakers, follows the Commerce Department's crackdown in October on the sale of advanced semiconductor chips to China for use in artificial intelligence and supercomputers. The administration also blacklisted a company that The Washington Post recently reported facilitated sales of U.S. technology to military institutes involved in China's hypersonics and missile programs. The moves come a month after President Biden and Chinese President Xi Jinping met in Bali and sought to put a "floor" under the downward spiraling relationship.

Read the full article here.

13 MAJOR CULTURAL DIFFERENCES BETWEEN CHINA AND THE UNITED STATES

Rebecca Graf | Owlcation | July 21, 2022

It is always interesting to study other cultures, and it is extremely important to do just that if you are going to have interactions with them. You don't want to insult someone or embarrass yourself and your own culture. China is one of those interesting cultures mainly because what we usually know about the country is through movies or the local Chinese restaurant. What I've learned over the years is that that knowledge is usually useless. A sincere study of a culture is the only way to truly appreciate the differences. So, being an American, what do I see as the 13 biggest cultural differences between the two countries? It took a long time to narrow it all down since we could get so detailed that an encyclopedia would be the end result.

Read the full article here.

RISE OF OPEN-SOURCE INTELLIGENCE TESTS U.S. SPIES

Warren P. Strobel | The Wall Street Journal | December 11, 2022

WASHINGTON—As Russian troops surged toward Ukraine's border last fall, a small Western intelligence unit swung into action, tracking signs Moscow was preparing to invade. It drew up escape routes for its people and wrote twice-daily intelligence reports. The unit drafted and sent to its leaders an assessment on Feb. 16, 2022, that would be eerily prescient: Russia, it said, would likely invade Ukraine on Feb. 23, U.S. East Coast time. The intelligence shop had just eight analysts and used only publicly available information, not spy satellites and secret agents. It belonged to multinational chemicals company Dow Inc., not to any government. "I'm leading an intelligence center that accurately predicted the invasion of Ukraine without any access to sensitive sources," said John Robert, Dow's director of global intelligence and protection, whose unit helps the company manage business risk and employee safety.

Read the full article here.

IMPROVED EXPORT CONTROLS ENFORCEMENT TECHNOLOGY NEEDED FOR U.S. NATIONAL SECURITY

Gregory C. Allen, Emily Benson, and William Alan Reinsch | Center for Strategic and International Studies December 5, 2022

As technology has become increasingly central to strategic competition with Russia and China, export controls have moved to the forefront of U.S. foreign policy on technology issues. Most notably, restricting Russia's access to advanced technology through export controls is a key part of the U.S. response to Russia's invasion of Ukraine, as U.S. government officials have repeatedly stated. Unfortunately, nearly all the debate is focused on whether and when to apply export controls, not how to ensure that export controls are effectively administered and enforced once applied. The Bureau of Industry and Security (BIS) at the Department of Commerce oversees most export controls. Unfortunately, BIS is increasingly challenged by worldwide smuggling and export control evasion networks, especially those that are supported by Russia and China.

Read the full article here.