ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

March 17, 2021

"NEVERNIGHT CONNECTION" AND "KNOW THE RISK, RAISE YOUR SHIELD"

National Counterintelligence and Security Center | March 10, 2021

Interested in training your personnel on threats like social media deception, social engineering, human targeting, & spear phishing? The National Counterintelligence and Security Center (NCSC) has a host of videos and other resources on its website (www.ncsc.gov) for companies and other stakeholders to use for educational purposes. The "Nevernight Connection," a recent movie by the FBI and NCSC, highlights how foreign intelligence services often use fake social media profiles to connect to people in industry or government who have access to information they want. See: https://lnkd.in/d6f35iP or visit: https://lnkd.in/d5x88uJ. NCSC also offers a host of "Know the Risk, Raise Your Shield" awareness videos that address additional threat scenarios your employees could face on any given day at home or work. For links to the full list of "Know the Risk, Raise Your Shield" awareness materials see: https://lnkd.in/dkzcXTY

Read the full article here.

WHITE HOUSE WARNS ORGANIZATIONS HAVE 'HOURS, NOT DAYS' TO FIX VULNERABILITIES AS MICROSOFT EXCHANGE ATTACKS INCREASE

Brian Fung and Alex Marquardt | CNN Politics | March 13, 2021

The Biden administration warned Friday that organizations face enormous risks from the recently disclosed Microsoft Exchange vulnerabilities that have affected thousands of private organizations. As attacks leveraging the vulnerabilities have escalated, the window for updating exposed servers is incredibly short -- "measured in hours, not days," a senior administration official told reporters. President Joe Biden was briefed on the Exchange hacks earlier this week, the official said. "He was very engaged on this topic, he asked a lot of questions on this topic and made clear that he directed that we address cybersecurity vulnerabilities and that we take on this topic with seriousness of purpose," the official told reporters. For the first time, the US government has invited members of the private sector to participate in the multi-agency task force established in reaction to the server software flaws, the official said. Private entities will be given access to sensitive compartmented information facilities around the country in order to participate in classified discussions where necessary, the official added.

Read the full article here.

FIVE CHINESE COMPANIES POSE THREAT TO U.S. NATIONAL SECURITY: FCC

David Shepardson | Reuters | March 12, 2021

The Federal Communications Commission (FCC) on Friday designated five Chinese companies as posing a threat to national security under a 2019 law aimed at protecting U.S. communications networks. The FCC said the companies included Huawei Technologies Co, ZTE Corp, Hytera Communications Corp, Hangzhou Hikvision Digital Technology Co and Zhejiang Dahua Technology Co. A 2019 law requires the FCC to identify companies producing telecommunications equipment and services "that have been found to pose an unacceptable risk to U.S. national security." Acting FCC Chairwoman Jessica Rosenworcel said in a statement: "This list provides meaningful guidance that will ensure that as next-generation networks are built across the country, they do not repeat the mistakes of the past or use equipment or services that will pose a threat to U.S. national security or the security and safety of Americans."

Read the full article here.

REMEDIATING NETWORKS AFFECTED BY THE SOLARWINDS AND ACTIVE DIRECTORY/M365 COMPROMISE

Cybersecurity and Infrastructure Security Agency

Since December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) has been responding to a significant cybersecurity incident affecting networks of multiple U.S. government agencies, critical infrastructure entities, and private sector organizations. Although the malicious activity varied among affected entities, an advanced persistent threat (APT) actor targeted and gained long-term access to select organizations' enterprise networks and moved laterally to Microsoft cloud systems—i.e., Azure Active Directory (AD) and Microsoft 365 (M365) environments. The actor used privileged access to collect and exfiltrate sensitive data and created backdoors to enable their return. CISA is providing the guidance below to support federal departments and agencies in evicting this threat activity from compromised on-premises and cloud environments. This guidance addresses tactics, techniques, and procedures (TTPs) leveraged by the threat actor.

Read the full article here.

MALICIOUS ACTORS ALMOST CERTAINLY WILL LEVERAGE SYNTHETIC CONTENT FOR CYBER AND FOREIGN INFLUENCE OPERATIONS

Federal Bureau of Investigation | March 10, 2021

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA. This PIN has been released TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. Malicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months. Foreign actors are currently using synthetic content in their influence campaigns, and the FBI anticipates it will be increasingly used by foreign and criminal cyber actors for spearphishing and social engineering in an evolution of cyber operational tradecraft.

Read the full article here.

FIREEYE CEO: RECKLESS MICROSOFT HACK UNUSUAL FOR CHINA

Frank Bajak and Nathan Ellgren | Associated Press | March 9, 2021

Cyber sleuths have already blamed China for a hack that exposed tens of thousands of servers running Microsoft's Exchange email program to potential hacks. The CEO of a prominent cybersecurity firm says it now seems clear China also unleashed an indiscriminate, automated second wave of hacking that opened the way for ransomware and other cyberattacks. The second wave, which began Feb. 26, is highly uncharacteristic of Beijing's elite cyber spies and far exceeds the norms of espionage, said Kevin Mandia of FireEye. In its massive scale it diverges radically from the highly targeted nature of the original hack, which was detected in January. "You never want to see a modern nation like China that has an offense capability — that they usually control with discipline — suddenly hit potentially a hundred thousand systems," Mandia said Tuesday in an interview with The Associated Press.

Read the full article here.

ACADEMIC EXPORT CONTROLS ENFORCEMENT CASE: 5 THINGS UNIVERSITIES CAN LEARN

Dr. Jennifer Saak | Traliance | March 9, 2021

The Bureau of Industry and Security (BIS) under the U.S. Department of Commerce recently announced an administrative settlement of $54,000 with Princeton University for potential export violations that the university self-disclosed. What can the research compliance and academic community learn from this case? The root of the export controls enforcement case is that Princeton University did not have the required BIS export licenses before shipping various strains and recombinants of animal pathogens to various international destinations. These items were classified under export control classification numbers ECCNs 1C351, 1C352, and 1C353 on the Commerce Control List (CCL). Biological materials are on everyone's mind as international research collaborations continue with the mission of developing new COVID-19 vaccines to fight the pandemic. So the news of this enforcement case is indeed timely.

Read the full article here.

SENATORS INTRODUCE BILL CREATING TECHNOLOGY PARTNERSHIPS TO COMPETE WITH CHINA

Maggie Miller | The Hill | March 4, 2021

Senate Intelligence Committee Chairman Mark Warner (D-Va.) and a coalition of bipartisan senators on Thursday introduced legislation intended to help the U.S. create international partnerships on emerging technologies to better compete with China. The Democracy Technology Partnership Act would create an interagency office at the State Department tasked with coordinating partnerships among the U.S. and other democratic countries to promote research and set standards around emerging technologies such as quantum computing, artificial intelligence, 5G and semiconductors. In addition, the bill would create a $5 billion International Technology Partnership Fund to help support joint research among democratic nations and academia and industries within those countries. The legislation also calls for strategies to provide alternatives for nations that may be considering buying technology from authoritarian regimes. The legislation is overall intended to help democratic nations take a stand against competition from the Chinese Communist Party on emerging technologies. The nation is seen as one of the greatest threats to the United States on a number of fronts.

Read the full article here.

MICROSOFT EXCHANGE "HAFNIUM" HACK: RECOMMENDED STEPS

Rich Sylva | Optiv | March 10, 2021

On March 2, 2021 Microsoft Corporation announced that a well-organized China-based threat actor named "Hafnium" deployed targeted attacks against a number of US-based businesses currently hosting "on-premise" Exchange Servers using multiple previously-unknown zero-day vulnerabilities. Time is of the essence and action must be taken immediately to protect your data. We recommend the following short- and long-term steps. Typical zero-day attacks usually take place using a single vulnerability. However, widespread attacks by Hafnium (rumored to be state-run) have taken advantage of four previously unknown vulnerabilities in Microsoft's "on-premise" versions of Exchange Server. Tens of thousands of companies are at risk in the US and internationally. Time is of the essence and action must be taken immediately to protect your data.

Read the full article here.

UK UNIVERSITIES' CLOSENESS TO CHINA POSES RISKS, SAYS JO JOHNSON

Rachel Hall | The Guardian | March 8, 2021

The former universities minister Jo Johnson has warned of the "poorly understood" risks of increasingly close collaboration between UK universities and China. A study led by Johnson identified a significant increase in funding from China and collaboration with Chinese researchers over the past two decades, including in sensitive areas for national security and economic competition – such as automation, telecommunications and materials science – or in disciplines where collaboration may threaten freedom of speech. "The UK urgently needs to put in place a framework for this key relationship so that it will be able to withstand rising geopolitical tensions. Failure to do so risks real damage to our knowledge economy," said Johnson. "The UK needs to do a better job of measuring, managing and mitigating risks that are at present poorly understood and monitored." China is on track to overtake the US as the UK's main research partner after a tenfold increase in research partnerships, from 750 in 2000 to 16,267 in 2019, primarily in technology-related disciplines. In 20 subject areas, collaborations with China account for more than 20% of the UK's high-impact research, the study said.

Read the full article here.

SENATE APPROVES BILL TO TIGHTEN CONTROLS ON CHINA-FUNDED CONFUCIUS INSTITUTES ON U.S. UNIVERSITY CAMPUSES

Christian Nunley | CNBC | March 6, 2021

The Senate on Thursday approved by unanimous consent — without a roll-call vote — a bill that would increase oversight on Confucius Institutes, China-funded cultural centers that operate on university campuses. According to Human Rights Watch, Confucius Institutes "are Chinese government-funded outposts that offer Chinese language and culture classes." However, some politicians, particularly Republicans, have accused them of spreading propaganda. "Confucius Institutes are under the control of the Chinese Communist Party in all but name," said Sen. John Kennedy, R-La., who introduced the bill. "This bill would give colleges and universities full control over their resident Confucius Institutes and restore freedom of thought on their campuses." In 2020, Sen. Marsha Blackburn, R-Tenn., introduced a similar bill. Sen. Marco Rubio, R-Fla., one of that bill's co-sponsors, said, "For far too long, the Communist Chinese government has attempted to infiltrate American universities through the disguise of the government-run Confucius Institute."

Read the full article here.

AI NOW MOST FAVORED MAJOR AT UNIVERSITIES

Zou Shuo | China Daily | March 3, 2021

Artificial intelligence has become the most popular new major at Chinese universities for the second year in a row amid the country's drive to build a strong AI talent pool. The subject's popularity is far above that of any other new major. A list issued by the Ministry of Education on Monday said universities across the country applied to establish 2,046 new majors last year, with 130 universities receiving approval to establish four-year undergraduate AI-related majors. In 2019, 180 universities set up AI majors, making it the No 1 new major in that year, too. Many prestigious universities—including Tsinghua University in Beijing, Sun Yat-Sen University in Guangzhou, Guangdong province, and Central South University in Changsha, Hunan province—are offering the new major.

Read the full article here.

CSU WILL CLOSE ITS CONFUCIUS INSTITUTE RATHER THAN RISK LOSS OF FEDERAL FUNDING

Paolo Zialcita | CPR News | March 6, 2021

A Colorado State University center partially funded by the Chinese government will close its doors later this year after Congress restricted funding for universities that host these programs. There are hundreds of Confucius Institutes across the globe. Named after the famed Chinese philosopher, CSU's Confucius Institute offers Chinese language and culture classes to the community at large. These education centers have faced bipartisan opposition in recent years, mainly due to its reliance on Chinese government funding. The 2021 National Defense Authorization Act, which passed Congress on New Year's Day after an override of a presidential veto, included language that restricted Department of Defense research funding at universities that host a Confucius Institute.

Read the full article here.

RESEARCHERS DEFINE KEY QUESTIONS TO HELP THE UK GOVERNMENT FOR NEXT BIOSECURITY THREAT

Emily Henderson | Medical Life Sciences News | February 4, 2021

During the summer of 2019, a global team of experts put their heads together to define the key questions facing the UK government when it comes to biological security. Facilitated by the Centre for Existential Risk (CSER) at the University of Cambridge and the BioRISC project at St Catharine's College, the group of 41 academics and figures from industry and government submitted 450 questions which were then debated, voted on and ranked to define the 80 most urgent. The final line-up includes major questions on future disease threats, including what role shifts in climate and land use might play, and whether data from social media platforms should be used to help detect the earliest signs of emerging pathogens.

Read the full article here.