ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

December 16, 2020

SUSPECTED RUSSIAN HACKERS SPIED ON U.S. TREASURY EMAILS - SOURCES

U.S. News | December 13, 2020

Hackers believed to be working for Russia have been monitoring internal email traffic at the U.S. Treasury and Commerce departments, according to people familiar with the matter, adding they feared the hacks uncovered so far may be the tip of the iceberg. The hack is so serious it led to a National Security Council meeting at the White House on Saturday, said one of the people familiar with the matter. U.S. officials have not said much publicly beyond the Commerce Department confirming there was a breach at one of its agencies and that they asked the Cybersecurity and Infrastructure Security Agency and the FBI to investigate. National Security Council spokesman John Ullyot added that they "are taking all necessary steps to identify and remedy any possible issues related to this situation." The U.S. government has not publicly identified who might be behind the hacking, but three of the people familiar with the investigation said Russia is currently believed to be responsible for the attack. Two of the people said that the breaches are connected to a broad campaign that also involved the recently disclosed hack on FireEye, a major U.S. cybersecurity company with government and commercial contracts.

Read the full article here.

MAJOR LEAK 'EXPOSES' MEMBERS AND 'LIFTS THE LID' ON THE CHINESE COMMUNIST PARTY

Sky News | December 13, 2020

A major leak containing a register with the details of nearly two million CCP members has occurred – exposing members who are now working all over the world, while also lifting the lid on how the party operates under Xi Jinping, says Sharri Markson. Ms Markson said the leak is a register with the details of Communist Party members, including their names, party position, birthday, national ID number and ethnicity. "It is believed to be the first leak of its kind in the world," the Sky News host said. "What's amazing about this database is not just that it exposes people who are members of the communist party, and who are now living and working all over the world, from Australia to the US to the UK," Ms Markson said. "But it's amazing because it lifts the lid on how the party operates under President and Chairman Xi Jinping".

Read the full article here.

STATE-BACKED HACKERS REPORTEDLY BREACH US TREASURY, COMMERCE DEPARTMENTS

Steven Musil | CNET | December 13, 2020

Hackers supported by a foreign government have been monitoring email at the US Treasury Department and a federal agency responsible for deciding internet and telecommunications policy, Reuters reported Sunday, citing unidentified sources familiar with the matter. Hackers who targeted the Treasury Department and the Commerce Department's National Telecommunications and Information Administration may also be targeting other agencies, the news agency reported. The National Security Council met at the White House on Saturday to discuss the hack, Reuters reported. "We can confirm there has been a breach in one of our bureaus," a Commerce spokesperson said. "We have asked CISA and the FBI to investigate, and we cannot comment further at this time." Hackers targeted the NTIA's office software, Microsoft's Office 365, monitoring staff emails at the agency for months, Reuters reported Microsoft declined to comment. Representatives for the FBI and the Treasury Department didn't immediately respond to requests for comment.

Read the full article here.

FIREEYE CONFIRMS SOLARWINDS SUPPLY CHAIN ATTACK

Catalin Cimpanu | ZDNet | December 14, 2020

Hackers believed to be operating on behalf of a foreign government have breached software provider SolarWinds and then deployed a malware-laced update for its Orion software to infect the networks of multiple US companies and government networks, US security firm FireEye said today. FireEye's report comes after Reuters, the Washington Post, and Wall Street Journal reported on Sunday intrusions at the US Treasury Department and the US Department of Commerce's National Telecommunications and Information Administration (NTIA). The SolarWindows supply chain attack is also how hackers gained access to FireEye's own network, which the company disclosed earlier this week. The Washington Post cited sources claiming that multiple other government agencies were also impacted. Reuters reported that the incident was considered so serious that it led to a rare meeting of the US National Security Council at the White House, a day earlier, on Saturday.

Read the full article here.

UW STATEMENT IN RESPONSE TO CLAIM BY US SECRETARY OF STATE MIKE POMPEO

University of Washington News | December 9, 2020

The following is a statement from the University of Washington in response to allegations U.S. Secretary of State Mike Pompeo made during a speech at Georgia Tech on Wednesday, Dec. 9, 2020: This is the latest false statement and shameful deflection from an administration whose State Department and Department of Education took no effective action on behalf of Vera Zhou in response to the University's requests, and now wishes to shift attention from that failure. That the Secretary of State would think a university has more power in this situation than the United States government is bizarre. That he would single out a staff member by name is unbecoming of the office and his statement is flatly wrong. While several UW offices have been in contact with Vera throughout her experience, no staff in the UW Office of Federal Relations has had direct contact with Vera or her family. The University of Washington has been deeply concerned for Vera's safety and well-being throughout her ordeal, and was relieved to hear of her safe return. We cannot even begin to imagine the turmoil this has caused in the lives of Vera, her mother and other loved ones.

Read the full article here.

FCC ORDERS EQUIPMENT REMOVED IN STEP AIMED AT HUAWEI, ZTE

Todd Shields | Bloomberg Quint | December 11, 2020

The Federal Communication Commission ordered carriers to remove network equipment that poses a security risk, taking another step aimed at China's Huawei Technologies Co. and ZTE Corp. The agency in a 5-0 vote also said it would establish a list of proscribed equipment, and it set up a program to reimburse carriers for replacing suspect gear that will start once Congress devotes an estimated $1.6 billion. The agency said the actions, which affect providers that take federal subsidies, implement a law Congress passed in March. The FCC, Congress and President Donald Trump's administration are confronting China on a range of issues including trade and the novel coronavirus. The FCC accuses Huawei and ZTE of posing a risk of espionage, an allegation each denies. Last year the agency said subsidies can't be used to buy gear from Huawei or ZTE. "The record on this is clear," said FCC Commissioner Brendan Carr, a Republican. "The Chinese government intends to surveil persons within our borders, for government security, for spying advantage, as well as for intellectual property and an industrial or business edge."

Read the full article here.

FLORIDA HOUSE TARGETS CHINESE INTERFERENCE IN HIGHER EDUCATION

Tampa Bay Times | December 15, 2020

Florida lawmakers will consider legislation to protect state universities and research institutions from interference by China, state House Speaker Chris Sprowls, R-Palm Harbor, said Tuesday. In a tweet, Sprowls said the legislation will come as part of efforts by the House Select Committee on the Integrity of Research Institutions, which was set up by former Speaker Jose Oliva in response to reports of Chinese meddling at Moffitt Cancer Center and at the University of Florida. "The Florida House launched the 1st State-initiated investigation into China's coordinated effort to access our Universities & research," Sprowls tweeted. "Next year, we will propose new legislation to make Florida the national leader in protecting our research institutions." The Tampa cancer center, which receives state funding, went through a shake-up after the center's chief executive officer, a senior member of the center and four researchers resigned over alleged violations of conflict-of-interest rules related to work in China.

Read the full article here.

POMPEO CRITICIZES COLLEGES OVER CHINA TIES

Elizabeth Redden | Inside Higher Ed | December 10, 2020

Secretary of State Mike Pompeo warned of Chinese government influence on American campuses and accused university leaders of censoring themselves out of fear of offending China during a speech Wednesday at the Georgia Institute of Technology. Pompeo said, "The Chinese Communist Party is poisoning the well of our higher education institutions for its own ends." The speech was notable for the strident tone taken by the nation's chief diplomat, even if its influence was arguably limited given his lame-duck status. The outgoing secretary of state addressed issues including intellectual property theft and recruitment of American professors into Chinese government-sponsored talent recruitment programs. He also raised concerns about Chinese students who fear speaking openly on American campuses lest they or their families be harassed, or worse. He further accused U.S. universities of censoring themselves or even overlooking illegal behavior to avoid offending China. He said many had been "bought by Beijing."

Read the full article here.

SECURITY IMPLICATIONS OF FOREIGN FUNDING AND ACCESS AT U.S. COLLEGES AND UNIVERSITIES

Kaylee Cox Bankston, Richard Hartunian, Scott Lashway, & Matthew Stein | JD Supra | December 9, 2020

While global media outlets have focused attention on election security, major U.S. healthcare facilities have been under direct cyberattacks in recent months. This follows disruptive cyberattacks on municipalities earlier this year. These attacks, and the often short news cycles around them, underscore the reactive attention to threats and the inability to foresee or prepare for emerging threats. Too often, industry verticals and their participants use the "not us, we're too small" approach to security preparedness. The next emerging threat—which in our view is already present—is to U.S. higher education, a big business due to its ability to generate new industries and technology from the ground up (e.g., social media). Like healthcare facilities and research organizations, higher education institutions and their electronic infrastructure are built for collaboration, which exposes a soft underside to threat actors. This presents serious security risks to the U.S. higher education sector and, in a larger sense, to U.S. national security interests.

Read the full article here.