CIPB-23-012 DISSEMINATED: 03 JANUARY 2023 DATE OF INFORMATION: 23 DECEMBER 2022

DCSA COUNTERINTELLIGENCE DIRECTORATE

CLEARED INDUSTRY REVIEW

WARNINGS:

The use of the linked articles and press releases in this publication does not constitute or imply an official endorsement of the content of these articles or of any news organization or media outlet. The Defense Counterintelligence and Security Agency (DCSA) is not responsible for the content of any of the linked news articles and cannot guarantee the accuracy of the information they provide. Any views or opinions expressed in these articles do not necessarily reflect those of DCSA, the Department of Defense (DOD), or the U.S. Government. Further reproduction or distribution of any linked news article appearing in this publication is subject to original copyright restrictions. Spelling variations contained in this review are direct quotes from the authors of the included published articles.

Operators of the websites linked in this product may have modified, removed, or restricted access to the websites subsequent to the date of its publication. When accessing links and websites, users should practice appropriate safe-browsing precautionary measures. Spelling variations contained in this review are direct quotes from the authors of the included published articles. Please email any comments/concerns to dcsa.ncr.dcsa.mbx.ci-partnership-branch@mail.mil.

INTELLIGENCE COLLECTION

The following article(s) highlight acts of espionage, covert, overt, and non-traditional intelligence collection. Highlighting intelligence collection in foreign and domestic environments furthers the defense industrial base's understanding of foreign adversarial collection priorities, techniques, and approaches.

FORMER TWITTER EMPLOYEE SENTENCED TO MORE THAN THREE YEARS IN PRISON FOR SPYING FOR SAUDI ARABIA

SUMMARY: A former Twitter employee, found guilty of spying on users on behalf of the Saudi royal family, has been sentenced to three and a half years in prison. Ahmad Abouammo, a dual U.S.-Lebanese citizen, who helped oversee media partnerships for Twitter in the Middle East and North Africa, was part of a scheme to acquire the personal information of users, including phone numbers and birth dates, for a Saudi government agent.

PUBLICATION: CNBC

LINK: https://www.cnbc.com/2022/12/16/ex-twitter-employee-sentenced-to-over-3-years-in-prison-for-spying-for-saudi-arabia.html

INTELLIGENCE SUCCESSES

The following article(s) highlight intelligence service successes in detecting, deterring, and disrupting foreign intelligence collection and industrial espionage activities, domestically and internationally.

AUSTRIA SAYS IT SUSPECTS GREEK OF SPYING FOR RUSSIA

SUMMARY: Austria said it had identified a 39-year-old Greek citizen whom it suspects of spying for Russia, adding that the citizen is the son of a former Russian spy who was once stationed in Germany and Austria as a diplomat. Austria's Interior Ministry made the announcement in a statement after an investigation conducted by its domestic intelligence agency "in close international cooperation" with countries or institutions that it did not name.

PUBLICATION: Reuters

LINK: https://www.reuters.com/world/europe/austria-says-it-suspects-greek-spying-russia-2022-12-19/

CYBER ATTACKS

The following articles cover cyber-attacks attributed to known advanced persistent threat actors and the damage caused after infiltrating networks.

IRANIAN HACKING GROUP EXPANDS FOCUS TO U.S. POLITICIANS, CRITICAL INFRASTRUCTURE, RESEARCHERS FIND

SUMMARY: An Iranian hacking group known as TA453; previously thought to mainly focus on compromising academics, journalists, and human rights workers; now appears to have added U.S. politicians, critical infrastructure and medical researchers to its target list. According to the cybersecurity firm Proofpoint, TA453, also known as Charming Kitten, Phosphorous and APT42, is becoming an important tool for the Iranian government to carry out digital espionage campaigns in support of other operations.

PUBLICATION: Cyber Scoop

LINK: https://www.cyberscoop.com/iran-ta453-charming-kitten-phosphorus-hacking-bolton/

FBI CHARGES 6, SEIZES 48 DOMAINS LINKED TO DDOS-FOR-HIRE SERVICE PLATFORMS

SUMMARY: The U.S. Department of Justice (DOJ) announced the seizure of 48 domains that offered services to conduct distributed denial-of-service (DDoS) attacks on behalf of other threat actors, effectively lowering the barrier to entry for malicious activity. The DOJ also observed that millions of individuals were attacked using the DDoS-for-hire platforms and that over one million registered users of IPStresser.com, one of the stressor (or booter) services, conducted or attempted to carry out more than 30 million DDoS attacks between 2014 and 2022.

PUBLICATION: The Hacker News

LINK: https://thehackernews.com/2022/12/fbi-charges-6-seizes-48-domains-linked.html

HACKER CLAIMS BREACH OF FBI'S CRITICAL-INFRASTRUCTURE PORTAL

SUMMARY: A hacker who reportedly posed as the CEO of a financial institution claims to have obtained access to the more than 80,000-member database of InfraGard, an FBI outreach program that shares sensitive information on national security and cybersecurity threats with public officials and private sector actors who run U.S. critical infrastructure. The hacker obtained access to InfraGard's online portal by posing as the CEO of a financial institution, observing the vetting process was surprisingly lax.

PUBLICATION: The Washington Times

LINK: https://www.washingtontimes.com/news/2022/dec/14/hacker-claims-breach-of-fbis-critical-infrastructu/

CHINESE APT GROUP MIRRORFACE INTERFERES IN JAPANESE ELECTIONS

SUMMARY: The Chinese APT group MirrorFace attempted to influence the elections for the Japanese House of Representatives this year, an investigation has revealed. According to researchers at European IT security vendor ESET, the group used spear-phishing attacks on individual members of a political party. The group reportedly primarily targets media, defense contractors, think tanks, diplomatic organizations, and academic institutions, with the goal of spying on and exfiltrating files of interest.

PUBLICATION: Dark Reading

LINK: https://www.darkreading.com/attacks-breaches/chinese-apt-group-mirrorface-interferes-japanese-elections

EXPORT VIOLATIONS

The following articles cover export violations that can have a national security impact by violating sanctions, International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) restrictions, or other export controls. Export violations related to military technology can provide an adversarial nation with better resources and equipment that are otherwise difficult to obtain through domestic production.

MASSACHUSETTS MAN SENTENCED FOR WIRE FRAUD AND ILLEGALLY EXPORTING DEFENSE ARTICLES TO TURKEY

SUMMARY: Arif Ugur, 53, of Cambridge, Massachusetts, the sole managing partner of the Anatolia Group Limited Partnership (Anatolia), a domestic limited partnership registered in Massachusetts, was convicted for illegally exporting defense technical data to foreign nationals in Turkey in connection with the fraudulent manufacturing of parts and components used by the U.S. military, in violation of the Arms Export Control Act. Ugur contracted and shared drawings of the parts and technical specifications with a company in Turkey to make the parts and then passed them off to DOD as if they had been manufactured by Anatolia in the United States.

PUBLICATION: Department of Justice

LINK: https://www.justice.gov/opa/pr/massachusetts-man-sentenced-wire-fraud-and-illegally-exporting-defense-articles-turkey

EXCLUSIVE: THE GLOBAL SUPPLY TRAIL THAT LEADS TO RUSSIA'S KILLER DRONES

SUMMARY: The hundreds of Russian drones hovering ominously over the Ukrainian battlefield owe their existence to an elastic, sanctions-evading supply chain that often runs through a shabby office above a Hong Kong marketplace, and sometimes through a yellow stucco home in suburban Florida. The "Sea Eagle" Orlan 10 UAV is a deceptive, relatively low-tech and cheap killer that has directed many of the up to 20,000 artillery shells that Russia has fired daily on Ukrainian positions in 2022, killing up to 100 soldiers per day, according to Ukrainian commanders

PUBLICATION: Reuters

LINK: https://www.reuters.com/world/europe/global-supply-trail-that-leads-russias-killer-drones-2022-12-15/

SPECIAL CONTENT

The following bulletin(s) alert the defense industrial base of current domestic, foreign, and/or cyber-related threats.

STATE-SPONSORED ECONOMIC CYBER-ESPIONAGE FOR COMMERCIAL PURPOSES: TACKLING AN INVISIBLE BUT PERSISTENT RISK TO PROSPERITY

SUMMARY: This policy brief by the Australian Strategic Policy Institute highlights the increasing threat of state-sponsored cyber-enabled intellectual property theft and the risk it poses to G20 countries. At the national level, addressing the threat of economic cyber-espionage requires a combination of strengthened awareness, recognition, and outreach by national cybersecurity authorities and counterintelligence agencies to industries that produce and possess intellectual property critical to future.

PUBLICATION: The Australian Strategic Policy Institute

LINK: https://www.aspi.org.au/report/state-sponsored-economic-cyberespionage

---

Prepared by: The Defense Counterintelligence and Security Agency Office of Counterintelligence Partnership Branch prepared this product. For questions, please contact us on NIPR at dcsa.ncr.dcsa.mbx.ci-partnership-branch@mail.mil. We appreciate all consumer input and feedback.