MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

May 2024

- **Country Scans — United States • Israel • United Kingdom**
- **Cyberattack forces shutdown of Canadian pharmacy chain**
- **UNDP reports cyber breach**
- **Chinese cybercrime syndicate exposed in Zambia**
- **World-first Cyber Crime Index identifies global hotspots**
- **Germany announces a dedicated cyber branch in military**
- **South Korea mulls banning iPhones in defense establishments**
- **India File**

Country Scans

United States

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) took action against Hamas, targeting the leaders responsible for offensive cyber and unmanned aerial vehicle (UAV) operations, notably, Hudhayfa Samir 'Abdallah al-Kahlut (al-Kahlut) also known as "Abu Ubaida" who leads the cyber influence department of al-Qassem Brigades.[1]

The Department of Justice has also undertaken actions against Iranians involved in targeting U.S. companies. Reports indicate that Iranian nationals have been charged in the Manhattan federal court for their participation in a cyber-enabled campaign aimed at infiltrating U.S. government and private entities.[2]

The conservative think tank, The Heritage Foundation, disclosed that it encountered a cyberattack in April.[3] An individual familiar with the incident confirmed that measures were being taken at Heritage to address the cyberattack. However, it was uncertain at the time whether any data had been compromised.

In a significant effort to curb proliferation of commercial spyware, the US Department of State has decided to take action against individuals who have been involved in the development and sale of commercial spyware.[4]The visa restrictions are part of wider U.S. government initiative as a response to growing cases of human rights breach owing to the commercial spyware.

Israel

Israel's Justice Ministry announced that it is investigating a cyber incident following claims by hacktivists protesting the Gaza conflict that they successfully infiltrated the ministry's servers, accessing hundreds of gigabytes of data.[5]A group identifying itself as "Anonymous for Justice" has claimed responsibility for the breach, asserting that it obtained nearly 300 gigabytes of data. The group stated on its website its intention to persist in targeting Israel until it ceases operation in Gaza.

In a separate incident, an Iranian cyber group known as Handala claimed that it successfully breached Israel's radar systems and distributed hundreds of thousands of threatening text messages to Israeli citizens.[6] The group claims to have infiltrated the radar systems and sent out 500,000 text messages as part of its operation.

United Kingdom

A police investigation has been initiated following reports of Members of Parliament being targeted in a spear-phishing attack.[7] Security experts suspect that this incident might be an attempt to compromise parliamentary systems. According to reports, the 12 confirmed targets include three Members of Parliament, two political journalists, a broadcaster, four party staff members, a former Tory MP, and a manager of an all-party parliamentary group. Among the targets are individuals affiliated with both the Conservative and Labour parties.

The UK government has also introduced a law making a sexually explicit 'deepfake' image to be a new offence.[8]Under the new law, creating a sexually explicit deepfake, regardless of the intent to share it, but with the sole purpose of causing alarm, humiliation, or distress to the victim, will constitute a criminal offense.

The UK has become the first country to prohibit default guessable usernames and passwords on IoT devices.[9] However, the use of unique default passwords remains

permissible. The Product Security and Telecommunications Infrastructure Act 2022 (PSTI) introduces minimum-security benchmarks for manufacturers. According to the legislation, weak or readily guessable default passwords like "admin" or "12345" are expressly prohibited.

According to the UK Government's Cyber Security Breaches Survey 2024, half of UK businesses have reported a cyber incident or data breach in the past 12 months.[10]The annual report, which surveyed 2000 UK businesses and 1004 charities, revealed that large businesses were the most frequently targeted (74%), followed by medium-sized businesses (70%) and small businesses (58%).

Cyberattack forces shutdown of Canadian pharmacy chain

Canadian pharmacy and retail chain London Drugs has temporarily closed all its stores in response to a cybersecurity incident.[11] The company later confirmed that the closure was indeed due to a cybersecurity incident. Initially, they stated that there was no indication that the data of customers or employees had been affected. London Drugs neither confirmed nor denied whether the incident was a ransomware attack.

UNDP reports cyber breach

According to reports, The United Nations Development Programme (UNDP) is investigating an alleged ransomware attack that resulted in data theft.[12] In the last week of March, UNDP became aware that a data-extortion threat actor had illicitly obtained data, which includes human resources and procurement information. According to officials, the scope of the breach is yet to be ascertained. Despite UNDP's silence about the source of attack, the ransomware group, 8base added UNDP to its Tor leak site.

Chinese cybercrime syndicate exposed in Zambia

In Zambia, authorities have unveiled a "sophisticated internet fraud syndicate," resulting in the apprehension of 77 individuals, among them 22 Chinese nationals.[13] The multi-agency raid on a Chinese-operated company led to this significant breakthrough. The company hired Zambian individuals under the impression that they would work as call-center agents. During the raid, authorities confiscated equipment that enabled callers to conceal their locations, along with thousands of SIM cards. Golden Top Support Services, the focal point of the operation, has refrained from providing any comments on the allegations.

World-first Cyber Crime Index identifies global hotspots

After three years of extensive research, an international team of researchers has compiled the inaugural 'World Cybercrime Index,' identifying the primary global cybercrime hotspots by ranking the most significant sources of cybercrime at a national level.[14] The index reveals that a relatively small number of countries pose the greatest cybercriminal threat. Topping the list is Russia, followed by Ukraine, China, the USA, Nigeria, and Romania. According to the index's authors, this study will enable both the public and private sectors to concentrate their resources on key cybercrime hubs, thereby reducing expenditure on cybercrime countermeasures in countries where the issue is less significant.

Germany announces a dedicated cyber branch in military

Germany's defense minister unveiled a military restructuring plan in April, which includes the establishment of a new central command and the creation of a dedicated branch for cyber space.[15] This initiative builds upon the ongoing Bundeswehr overhaul initiated in response to Russia's invasion of Ukraine. The cyber space branch will specifically target hybrid threats such as disinformation campaigns.

South Korea mulls banning iPhones in defense establishments

South Korea's military is reportedly considering a complete ban on iPhones within military premises due to growing apprehensions regarding the potential leakage of sensitive information via voice recordings.[16] The proposal to prohibit iPhones within the military emerged from collaborative discussions held by the army, navy, and air force headquarters, according to reports. Interestingly, while iPhones are explicitly prohibited, Android-based devices manufactured by Samsung are exempt from the ban. Alongside iPhones, the ban reportedly extends to wearables such as the Apple Watch.

India File

- Personal data belonging to over 7.5 million customers of boAt, a renowned manufacturer of audio products and smartwatches, has surfaced on the dark web, available for purchase at a mere 2 euros.[17] The leaked information includes sensitive personal details such as names, addresses, contact numbers, email IDs, and customer IDs. The breach, totaling approximately 2GB of data, was revealed by a hacker on a prominent forum.
- According to reports, cyberattacks on Indian government entities by Pakistan-linked Advanced Persistent Threats (APTs) have escalated significantly.[18] One notable threat group, SideCopy, has recently conducted three distinct campaigns over several weeks, deploying their frequently used AllaKore Remote Access Trojan (RAT). India stands out as one of the most targeted countries in the cyber threat landscape. Notably, Pakistan-linked APT groups such as SideCopy and APT36 (Transparent Tribe) have been active in targeting India.
- The Indian government has announced the rescue of 250 citizens from Cambodia, where they were lured by job opportunities but ultimately coerced into perpetrating cyber fraud.[19]In response to media queries, the spokesperson for the Indian Ministry of External Affairs said that the Indian Embassy in Cambodia is actively responding to complaints from Indian national who were forced to do the illegal cyber work.[20]

[1] U.S. Department of the Treasury, Treasury Targets Hamas UAV Unit Officials and Cyber Actor, 12 April 2024, https://home.treasury.gov/news/press-releases/jy2248

[2] Office of Public Affairs, U.S. Department of Justice, Justice Department Charges Four Iranian Nationals for Multi-Year Cyber Campaign Targeting U.S. Companies, 23 April 2024, https://www.justice.gov/opa/pr/justice-department-charges-four-iranian-nationals-multi-year-cyber-campaign-targeting-us

[3] Techcrunch, US think tank Heritage Foundation hit by cyberattack, 12 April 2024, https://techcrunch.com/2024/04/12/heritage-foundation-cyberattack/

[4] U.S. Department of State, Promoting Accountability for the Misuse of Commercial Spyware, 22 April 2024, https://www.state.gov/promoting-accountability-for-the-misuse-of-commercial-spyware/

[5] Reuters, Israel's Justice Ministry reviewing 'cyber incident' after hacktivists' claim breach, 5 April 2024, https://www.reuters.com/world/middle-east/israels-justice-ministry-reviewing-cyber-incident-after-hacktivists-claim-breach-2024-04-05

[6] The Jerusalem Post, An Iranian cyber group claims: 'We breached the radars in Israel', 14 April 2024, https://www.jpost.com/israel-news/article-796869

[7] The Guardian, Police launch inquiry after MPs targeted in apparent 'spear-phishing' attack, 4 April 2024, https://www.theguardian.com/uk-news/2024/apr/04/police-launch-inquiry-after-mps-targeted-in-apparent-spear-phishing-attack

[8] GOV.UK, Government cracks down on 'deepfakes' creation, 16 April 2024, https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation

[9] The Record, UK becomes first country to ban default bad passwords on IoT devices, 29 April 2024, https://therecord.media/united-kingdom-bans-defalt-passwords-iot-devices

[10] Infosecurity Magazine, Half of UK Businesses Hit by Cyber-Incident in Past Year, UK Government Finds, 10 April 2024, https://www.infosecurity-magazine.com/news/half-uk-businesses-cyber-incident/

[11] SC Media, London Drugs pharmacy closes all stores to respond to cyber incident, 30 April 2024, https://www.scmagazine.com/news/london-drugs-pharmacy-closes-all-stores-to-respond-to-cyber-incident

[12] Security Affairs, United Nations Development Programme (UNDP) investigates data breach, 19 April 2024, https://securityaffairs.com/162025/cyber-crime/undp-investigates-data-breach.html

[13] BBC, Zambia uncovers 'sophisticated' Chinese cybercrime syndicate, 10 April 2024, https://www.bbc.com/news/world-africa-68777137

[14] University of Oxford, World-first "Cybercrime Index" ranks countries by cybercrime threat level, 10 April 2024, https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level

[15] Reuters, Germany announces military overhaul with eye on cyber threats, 4 April 2024, https://www.reuters.com/world/europe/germany-announces-military-overhaul-with-eye-cyber-threats-2024-04-04

[16] Firstpost, South Korea bans iPhones for military males but home-grown Samsung's Android phones are alright, 24 April 2024, https://www.firstpost.com/tech/south-korea-bans-iphones-for-military-males-but-home-grown-samsungs-android-phones-are-alright-13763332.html

[17] The Economic Times, boAt Data Breach: Name, address, contact number, email ID of 75 lakh boat customers for sale at 2 euro, 9 April 2024, https://economictimes.indiatimes.com/industry/cons-products/electronics/boat-data-breach-name-address-contact-number-email-id-of-75-lakh-boat-customers-reportedly-leaked-online/articleshow/109127405.cms?from=mdr

[18] Seqrite, Pakistani APTs Escalate Attacks on Indian Gov. Seqrite Labs Unveils Threats and Connections, 24 April 2024, https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/

[19] The Record, India says it has rescued 250 citizens from Cambodian cyber slavery, 1 April 2024, https://therecord.media/india-rescued-cambodia-scam-centers-citizens

[20] Government of India, MEA, Official Spokesperson's response to media queries regarding Indians stuck in Cambodia, 30 March 2024, https://www.mea.gov.in/response-to-queries.htm?dtl/37760/Official_Spokespersons_response_to_media_queries_regarding_Indians_stuck_in_Cambodia