Major Events and Trends in Cybersecurity in 2020

March 2021

The cybersecurity landscape was largely affected by the Covid-19 pandemic in 2020. There was an increased demand for digitised work, e-commerce, and people-to-people connectivity online. The pandemic was exploited by various cyber criminals throughout the year to mount attacks on a wide range of institutions, especially those on the supply chain, healthcare institutions, and organisations involved in vaccine research and distribution.

Nearly 700 million internet users were recorded in 2020 across India, with a projected number of 636 million internet users by 2021. With the growing number of internet users and an emerging market across the country, there has been an escalation of targeted cyber-attacks in various sectors. India **was** ranked as the second most cyber-attacked country in the Asia-Pacific region, after Japan, according to IBM Security's X-Force Threat Intelligence Index. Finance and insurance were the top cyber-attacked industries accounting for about 60 percent of the attacks, followed by manufacturing and professional services. Cyberattacks on healthcare, manufacturing and energy in 2020 doubled from the previous year.

The year saw a heavy dependence on the internet by healthcare institutions. The National Informatics Centre under the Ministry of Electronics and Information Technology (MeitY) developed the innovative Aarogya Setu app which has been used as a contact tracing, covid-19 related informational and self-assessment digital service for connecting the citizens with the government and curbing the spread of covid-19 in the country. Around 17.16 crore Indians have used the app. In a push towards the creation of Digital India, the Union Cabinet chaired by Prime Minister Shri Narendra Modi gave approval for setting up of public Wi-Fi networks through the Prime Minister Public Wi-Fi Access Network Interface (PM-WANI) scheme which would help in the proliferation of public Wi-Fi in the country.

2020 also saw a rapid expansion of digital payments. The National Payments Corporation of India (NPCI) UPI reached 1.49 billion in volume and US$41 billion in transaction value in July 2020. It is also estimated that India's digital economy may reach US$1 trillion by 2025. The rapidly expanding digital financial space has also given rise to financial fraud cases like fake buyer accounts, identity theft, card detail theft, etc. The remote working conditions too has made banks and financial institutes vulnerable to threats like never before.

There has been an increased reliance on third parties by businesses in recent years as they tend to outsource work in order to tackle any shortage of resources. Threat actors modified their attacks in 2020 with many of the attacks taking place on the supply chain. The attacks took place on organisations that are vulnerable and one step away from the main target. These kind of attacks often cause a ripple effect on organisations present in the entire chain.

One such attack and one of the biggest in 2020 was the massive cybersecurity breach of Solarwinds that was discovered by US cyber security company, FireEye. Almost 300,000 customers, 18,000 companies and agencies including government and private agencies were impacted. Trojanised versions of Solarwinds' Orion software was made available as a software update which the customers used to update their systems. The update contained a malware called 'sunburst', which was capable of accessing system files/information of client systems, which, in turn, gave hackers a backdoor entry. According to reports, parts of the Pentagon, Centres for Disease Control and Prevention, the Justice Department, and many others were victims of the attack. The US nuclear weapons agency and at least three states were also

hacked. Even Microsoft and several other big tech companies, Cisco, Intel, Nvidia, Belkin, and VMware had computers on their networks infected with the malware.

In December 2020, IBM reported that the vaccine supply chain linked to Gavi, the international vaccine alliance which helps distribute vaccines around the world, was targeted by cyber-espionage. The logistics network used to keep the vaccines at the right temperature during transportation, was targeted with malicious codes, via phishing emails. While the identity of the attackers was not apparent, the sophistication of their methods indicated a nation state, according to IBM.

Phishing campaigns, in general, have risen 'dramatically' since January 2020, according to the cyber security company, FireEye. 2020 saw Covid-19 driven phishing campaigns that were motivated by the urge for increased need of information on Covid 19-related topics and the subsequent rise in the number of websites that provide such information. Inimical actors specifically created websites with the intention to spread misinformation and malware.

Some hackers used 'socially-engineered' coronavirus-themed phishing emails 'crafted' with interesting facts on Covid-19, health and lifestyle advice, and information on vaccine development. Such sites contained malicious files which impersonated official websites and also asked for bitcoin donations to fund fake vaccines. According to Verizon's 2020 Mobile Security Index, smishing attacks have increased from 2 percent to 13 percent in just the past year.

Attacks on Remote Desktop Protocol (RDP) & Virtual Private Networking (VPN) were also on the rise throughout 2020. This was mainly due to the shift of office to the work-from-home mode. Since RDP and VPN allow access to corporate data and servers off-site, it gave cyber criminals the perfect ground to launch attacks on RDP, VPN and other remote services. Even though VPN provides an additional security layer, cybercriminals view VPN as a vulnerable point of entry to any organisation's network. It is predicted that there would be a further spike in the number of such attacks in the coming years. The attacks on VPN and RDP has almost doubled from last year.

Another major concern throughout 2020 was with regard to employees working from home who use devices that are not patched and not secured properly by the organisations. Many organisations have permitted employees use of own devices in order to overcome the challenges of remote work. The data from these devices gets stored in the cloud servers and these data often contain sensitive company information. Employees in general are not skilled enough in cloud security. As cloud adoption continued to grow in 2020, hackers have used this route to launch cyber-attacks on several organisations.

Moreover, home routers are often not properly secured and vulnerable for attacks. Inadequate security controls also put other Internet of Things (IOT) devices in the same network under risk. January 2020 saw MVPower DVR Remote Code Execution as the most common exploited vulnerability, impacting 45 per cent of organisations globally. It is a remote code execution vulnerability in MVPower DVR devices. A remote code execution vulnerability was also reported in 'D-Link DSL-2750B routers' under top exploited vulnerabilities in 2020.

The top malware threats at the beginning of the pandemic included Emotet (an advanced Trojan that uses multiple evasion techniques to avoid detection) which was distributed as a coronavirus-themed messages in Japan, and Lokibot, which targeted users in

Indonesia. xHelper (a malicious application), Guerilla (an Android Trojan) and AndroidBauts (adware targeting Android users) were the most prevalent mobile malware in the beginning of 2020. Some of these are capable of downloading other malicious apps while some of them hide from the user and reinstall themselves, if uninstalled.

An Interpol assessment has found out that from January to April 2020, nearly 50,000 malicious URLs related to Covid-19 were detected. An estimated loss of nearly £970,000 was reported by Action Fraud, UK's national fraud and cybercrime reporting centre, due to coronavirus-related reports since February 1, 2020. According to Barclays' data, scams went up to 66 per cent in the first six months of 2020 in the UK. The scams also included cryptocurrency frauds, especially during the lockdown. The nature of threats have also transformed in recent years. A few years back, cyber-attacks mainly took place by lone hackers who were involved in minor frauds like misuse of personal information. Today, cyberattacks have turned into organized crimes with large gangs of cyber criminals who are highly-trained developers and who are a potential threat to nations.

Citing disruptions in services, a global outage of Google services occurred for approximately 47 minutes on December 14, 2020 which disrupted core services like Gmail, Google Drive, Google Docs, Google Meet, and Google voice. Soon after, Google released a report mentioning the cause of the outage as an issue in its authentication platform. A second outage also occurred the next day, in which the Gmail service was down for two hours. An abrupt disruption of Google services had also occurred earlier in November 2020.

A good progress was seen with respect to cybersecurity in India when the National Security Council Secretariat (NSCS) in December 2020 issued a call for public comments in order to formulate a National Cyber Security Strategy (NCSS) for 2020-2025. This move was aimed at ensuring a safe, secure, trusted, resilient and vibrant cyber space. After the National Cyber Security Policy (2013), which has so far guided the government in securing the cyberspace, this move was a progressive one keeping in mind the rapid technological developments that took place in the recent years. As the government continues to embrace IoT-enabled solutions to achieve automation and efficiency, there needs to be an increased focus across stakeholders on securing the IoT infrastructure, especially of critical infrastructure and smart cities.

CERT-In in 2020 successfully conducted the 'Black Swan–Cyber Security Breach Tabletop Exercise' to deal with cyber crises and incidents emerging due to COVID-19 pandemic due to lowered security controls. The objectives of the exercise was to deal with Covid-19 related cyber-attacks when attackers used Covid-19 themed attacks. The government also considered setting up of a Computer Emergency Response Team for the Financial Sector (CERT-Fin) with expertise from various financial sector agencies such as the ministry of corporate affairs (MCA), the Employees Provident Fund Organization (EPFO), the Serious Fraud Investigation Office (SFIO), the Security Printing and Minting Corporation of India Limited (SPMCIL) and the Goods and Service Tax Network (GSTN) to protect the country's financial sector. Prime Minister Modi also announced a new cybersecurity policy for safe and secure cyberspace in India on the Independence Day. Tamil Nadu in September 2020 became the first Indian state to come up with policies on ethical intelligence, cybersecurity and blockchain.

New security challenges were seen in 2020 with the rapid deployment of tools and technologies that enabled remote work. There were increased security concerns among nations from the previous year and a global rift between political, economic, and social issues mainly linked to the pandemic.

Investigations by cyber experts in September 2020 revealed that a Chinese firm had designed and deployed tools to monitor at least 10,000 Indians, including top level officers. These tools used Artificial Intelligence (AI) to mine data and track movements from a person's digital presence which was in turn used to monitor them. The firm was closely associated with intelligence, military and security agencies of China. When both India and China were facing serious border conflicts last year, this incident could be considered as part of a psychological warfare aimed at influencing domestic policies. In the near future, security innovation and more capable and smart solutions like AI and machine learning can be applied in government and private organisations to boost cyber defences.

2020 also witnessed a 'technological Cold War' between the United States (US) and China which was highlighted by the US' cut off of Huawei's access to advanced computer chips and the banning of other Chinese companies. Washington had alleged that Huawei products threatened national security as they could be used to spy on Americans, though Huawei has repeatedly denied such allegations.

The Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), set up by the UN in 2018, submitted its report in March 2021. It ran in parallel with the Group of Governmental Experts (GGE) on Advancing responsible State Behaviour in Cyberspace. The OEWG report identified existing and potential threats at varied levels that states experience according to its levels of digitalisation, capacity, ICT security and resilience, infrastructure and economic development.

Conversely, there has been an increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups. The report dwelt on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, particularly emphasising the protection of healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure. Confidence-building measures (CBMs) can strengthen the overall security, resilience and peaceful use of ICTs. CBMs can also support implementation of norms of responsible state behaviour. The mandate for the OEWG was renewed in December 2020 for a further five years, and taken in conjunction with the recommendation for regular institutional dialogue, more substantive recommendations may be expected, going forward.

Sectoral Analysis of Key Cybersecurity incidents in 2020

The major critical infrastructures in 2020 shifted to the digital arena due to the Covid-19 pandemic. The interconnectedness of different sectors of the government exposed critical infrastructure to increased risk. For example, the medical research laboratories developing vaccines are now a part of critical infrastructure. Healthcare facilities were the most desirable targets for ransomware attacks. Cybersecurity threats facing operation technology (OT) and

industrial control systems (ICS) were also recorded, with most of the incidents suspected to be linked to state actors.

Critical Information Infrastructure

Israeli officials in 2020 had confirmed that a cyberattack was attempted on its water systems to alter the treatment chemicals to unsafe levels. It was suspected to be linked to Iranian cyber actors. In May 2020, the Iranian port of Shahid Rajaee suffered a significant cyberattack causing serious disruption of port traffic. Officials characterised the attack as a retaliation against the previous incident.

In February 2020**,** the U.S. Defense Information Systems Agency announced it had suffered a data breach exposing the personal information of an unspecified number of individuals**.** In the same month, Mexico's Economy Ministry announced it had detected a cyber-attack launched against the ministry's networks, but that no sensitive data had been exposed. Japan's Defense Ministry also announced in February 2020 that a large-scale cyber-attack against Mitsubishi Electric had taken place that could have compromised details of new state-of-the-art missile designs.

Political Espionage

In December 2020, Facebook had announced that its users had been targeted by two hacking campaigns, one originating from state-sponsored Vietnamese hackers and the other from two non-profit groups in Bangladesh. The first one was aimed at spreading malware and the second was focused on compromising accounts. Suspected Chinese hackers targeted government agencies and the National Data Center of Mongolia as part of a phishing campaign in the same month.

In October 2020, the UK's National Cyber Security Centre claimed that it found evidence of Russian military intelligence hackers planning a disruptive cyber-attack on the 2020 Tokyo Olympics (which was postponed). According to reports, Russian hackers had also targeted government agencies in NATO member countries in the month of September 2020. The campaign was mainly a phishing campaign that used NATO training material as phishing emails. Earlier in April 2020, suspected Vietnamese hackers had used malicious apps in the Google Play app store. It affected around 300 devices of users in Vietnam, India, Bangladesh, Indonesia, Iran, Algeria, South Africa, Nepal, Myanmar, and Malaysia by infecting them with spyware capable of monitoring their digital data.

Industrial Espionage

In October 2020, the pharmaceutical company, Dr. Reddy's Lab, was the victim of a cyber-attack. After a data breach was reported in its servers, the company had to shut down its plants and isolate its data centres across the world, to contain the attack. The company centre in India is the contractor for Russia's 'Sputinik V' Covid-19 vaccine. In November 2020, state-sponsored hackers from China, Russia, Iran and North Korea attempted to steal valuable vaccine secrets, by targeting British drug maker AstraZeneca. The hackers approached AstraZeneca staff with fabricated job descriptions laced with malicious codes. In December 2020, a criminal group

targeted the Israeli insurance company Shirbit with ransomware demanding almost US$1 million in bitcoin. The hackers had revealed sensitive personal information that was obtained from the company following a data breach.

Electoral Process

The US Cyber Command and the NSA conducted an operation against Iran aimed at identifying malicious cyber actors to protect the 2020 US elections and prevent any foreign interference in it. The US government had also announced that Iranian hackers targeted state election websites in order to download voter registration information and conduct a voter intimidation campaign. In July 2020, the UK announced that it believed Russia had attempted to interfere in its 2019 general election by stealing and leaking trade documents. According to Microsoft, cyber-attacks targeting people and organizations involved in the US presidential election were detected in 2020. The attacks, though unsuccessful, were mostly targeted attacks on people associated with both the Trump and the Biden campaigns.

Major Cyber incidents in the South Asian region

India

In a major data breach, Twitter, the popular microblogging platform became victim of a phone spear-phishing attack in July 2020. The attackers used the credentials of the Twitter employees in which almost 130 accounts were apparently compromised. In another data breach, data from more than 500,000 Zoom accounts were sold on the dark web.

Marriott International, the multinational diversified hospitality company had also faced a massive data breach in January 2020, in which data containing personal information of around 5.2 million guests was compromised. It included information like names, mailing addresses, contact details, etc.

Juspay confirmed the August 2020 data breach after an investigation revealed unauthorised access by hackers on a server that formed part of its payment system. The data breach affected 35 million customer accounts with masked card data and card fingerprints. Details of close to 35 million customer accounts, including masked card data and card fingerprints, were taken from a server using an unrecycled access key.

Pakistan

In 2020, Pakistan's Higher Education Commission was attacked by scammers. Later on, the clarification was made by HEC that someone wanted to make changes in its HTML coding by uploading a screenshot of the website which made it seem like a hack. Connectivity issues still remain a problem in parts of Balochistan, Gilgit Baltistan and some districts of Punjab, according to student unions.

An intrusion also occurred during a webinar at the Institute of Strategic Studies due to the use of a non-encrypted internet connection. The Pakistan military in August 2020 claimed that intelligence authorities had detected a cyber-attack by Indian intelligent forces in which the mobile phones of several Pakistani government officials and military personnel were hacked. During the same time period a suspected Pakistan-backed hacker group called Transparent Tribe used phishing emails to extract sensitive information from Indian defence personnel.

Bangladesh

In August 2020, the Bangladesh government's Computer Incident Response Team (CIRT) had informed the central bank about a cyber-attack attempt by the North Korea-based hacker group called Beagle Boys. The Financial Institutions Division of the Finance Ministry of Bangladesh had warned the banks regarding cyber security threats and asked them to strengthen their online security measures. The country's internet banking services witnessed greater volume of business amidst the pandemic as the sector shifted from traditional banking to digital banking.

On February 5, 2016, Bangladesh faced one of the biggest cybercrimes in the world when unidentified hackers had stolen US$101 million from Bangladesh Bank's account with the Federal Reserve Bank of New York, using fake orders on the SWIFT payment system. According to a survey involving banking, insurance, telecom and manufacturing enterprises, an approximate 72 per cent of Bangladesh organisations saw ransomware as a key cybersecurity challenge, while 70 per cent saw phishing scams as a top challenge.

Sri Lanka

A series of cyberattacks took place on at least 5 Sri Lankan national websites with the top-level domains in the month of May 2020. The attacks also took place on a leading news website of Sri Lanka, on a diplomatic mission and several private and state entities. The cyber-attack was believed to be conducted by a group called 'Tamil Eelam Cyber Force'. With the Information and Cyber Security Strategy of Sri Lanka (2019 – 2023), Sri Lanka Computer Emergency Readiness Team (SLCERT) plans to cooperate and create more public-private and local-international partnerships in the coming years.

Bhutan

Bhutan's national computer incident response team, Bhutan Computer Incident Response Team (BtCIRT), flagged an increase in cyberattacks in 2020 which led to major damage in terms of financial and data loss and service disruptions to individuals and companies. The BtCIRT team also observed a lot of social media phishing and showed concern regarding educating people about cyber hygiene and safety. The Overseas Security Advisory Council (OSAC) in its Bhutan 2020 Crime & Safety Report highlighted some best practices for maximizing security on public Wi-Fi.

Nepal

On March 2020, hackers leaked a database consisting of more than 50,000 user names, their personal details, current address, emails, and phone number following a databreach of Foodmandu, an e-commerce firm delivering on-demand food distribution services throughout the Kathmandu region. The company later published an apology letter to their customers for the same. A similar data breach happened just a month later, in which the personal details of around 170,000 Vianet (one of Nepal's leading Internet Service Providers) customers were leaked onto the internet. The breach was announced by anonymous hackers via Twitter.

***

Published by:
MP-IDSA Cybersecurity Centre of Excellence,
Manohar Parrikar Institute for Defence Studies and Analyses,
1, Development Enclave, (near USI), New Delhi, Delhi 110010
Email: iccoe.idsa@gov.in