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

CYBER *Digest*

April 2021

- Pimpri Chinchwad Smart City servers hit by Ransomware
- Cyberattacks on critical sectors double over 2019 in India
- Indian companies attacked using Microsoft server vulnerabilities
- Google plans to stop selling ads based on individuals' browsing
- Grab partners with Indonesian govt. for vaccination drive
- China's 'Sharp Eyes' Program close to 100% surveillance
- RBI orders Mobikwik audit after data breach
- UN OEWG on ICT developments submits report

Prepared by: Ms. Debopama Bhattacharya

Pimpri Chinchwad Smart City servers hit by Ransomware

The servers of a smart city, the Pimpri Chinchwad Municipal Corporation in Pune were hit by a ransomware attack on February 26th 2021. The smart city project is managed by the multinational technology company, Tech Mahindra. Though there was no data loss in the attack, reportedly, the attackers had demanded that the ransom be paid in bitcoins.[1]

A detailed analysis of the situation by Tech Mahindra has concluded that at least 25 servers were impacted and would have to be rebuilt again along with a robust security system which would cost an estimated 5 crores for the rework efforts.

As per the latest reports, political parties have demanded a probe into the whole matter after Tech Mahindra asked Pimpri Chinawada to recover the losses in a police complaint.[2] Despite Pimpri Chinawada spending crores of rupees on the smart city project, this incident has raised questions on whether the data is safe or not.

Cyberattacks on critical sectors double over 2019 in India

IBM Security has released the 2021 X-Force Threat Intelligence Index highlighting the major cybersecurity threats in 2020.[3] India has been the second most cyber-attacked country in the Asia-Pacific region after Japan, according to the report.

Attacks on India made up 7% of all attacks in the Asia-Pacific region in 2020. Finance and insurance were the top attacked industries in India with about 60 percent of the attacks, followed by manufacturing and professional services. Cyberattacks on healthcare, manufacturing and energy doubled from 2019.

Ransomware was the top cyber threat which comprised of 40 percent of attacks, sodinokibi (REvil) being the most common type. Other threats included data theft, remote access trojans (RAT), common vulnerabilities and exposure (CVE) and business email compromise (BEC).[4]

Another important observation in the report was the new trend in which data theft from data breaches, and ransomware attacks happened simultaneously. This led to a double extortion strategy from ransomware attacks in which attackers encrypted and stole the data at first, and then threatened to leak the data in case of denial of the ransom.[5]

The Threat Intelligence Index is made from the data observations across 130 countries and monitoring over 150 billion security events per day.

Indian companies attacked using Microsoft server vulnerabilities

After Microsoft announced the discovery of serious vulnerabilities in its Exchange software on March 2, 2021, hackers since then have become active all over the world to exploit the vulnerabilities in the exchange software. Recent reports have stated that at least 32 Indian organisations were the victims of cyber-attacks following the announcement made by Microsoft.[6]

The finance and banking institutions in India were the most-affected, followed by government and military organisations, manufacturing, insurance and others, according to Check Point Research. The country which was most attacked was the US, followed by The Netherlands and Turkey.

Microsoft had soon after declared that it would release fixes for the security flaws in the email software and released an emergency patch for its Exchange Server product on March 3rd, but even then many organisations worldwide could barely manage to patch their software in such a short time which left them exposed to vulnerabilities.

Microsoft has also detected a new family of ransomware called the 'DearCry,' which was being used after an initial compromise of unpatched on-premises Exchange Servers. Researchers from the cybersecurity firm have stated that security professionals are using massive preventative efforts to combat all kinds of hacking attempts.

Google plans to stop selling ads based on individuals' browsing

In a move towards maintaining more digital privacy, Google plans to stop selling ads based on individuals' browsing across multiple websites by the next year. Google has also stated that it is time that digital advertising evolves in order to address the growing concerns people regarding data privacy and tracking.

According to a blog post of Google, tracking individual's browsing history is not sustainable for a long term investment.[7] Therefore, it is looking for newer and smarter methods like privacy preserving Application Programming Interfaces (APIs) that will deliver the same results while protecting individual privacy. The search giant last year had also declared that it would phase out third-party cookies[8] eventually which would further prevent data tracking for advertisers and websites.

However, Google also stated that these changes would not apply to the 'first party' data, the ones which companies collect directly from consumers. Google's own products, like Gmail, YouTube and Chrome are also included in this. The changes will also apply to websites only and not mobile phones.[9]

Google's search and targeted advertising business has been repeatedly attacked by lawmakers and state and federal prosecutors in recent years. Currently the company faces some major antitrust lawsuits from various governments- including one by the US Department of Justice.[10]

Grab partners with Indonesian govt. for vaccination drive

Grab, the multinational ride-hailing company of Southeast Asia, has partnered with the Indonesian government and the medical app Good Doctor to open a drive-through vaccination centre in Bali.[11] The move is aimed at helping the nation inoculate its citizens with COVID-19 vaccines. Grab and Good Doctor have additionally also provided their digital infrastructure to allow citizens to pre-register for the vaccine in the drive-through line at the centre.

The first Grab vaccine center in Bali plans to vaccinate drivers in the transportation sector, including Grab drivers and delivery-partners and public sector workers from the tourism sector in Bali. Grab also plans to build more drive-through vaccination centers in other cities.

The vaccination drive works through an invitation via a text message from the government or a message on the Grab driver-partner app. It is mandatory for those who receive the invitation to take the vaccination.

Grab, with the support of doctors from Good Doctor is also working with the government to use its platform to educate users regarding COVID-19 vaccine and combating misinformation. According to the Indonesian government, the need to collaborate with the private sector is a necessary step to accelerate the vaccination exercise in the country.[12]

China's 'Sharp Eyes' Program close to 100% surveillance

The 'Sharp Eyes' surveillance program, which was initiated in 2013 in the region of Pingyi County in China, is close to achieving 100 per cent surveillance of public spaces now throughout the country.[13] This unique surveillance program allows citizens to monitor security camera footages with the help of special TV boxes installed in their homes and report anything suspicious to the police. The footages are also monitored by automated facial recognition algorithms.

Under the project, an area is divided into grids and each square of the grid acts as an administrative unit. Cameras are installed in each grid for surveillance by citizens as well as the authorities.

'Sharp Eyes' is one among several other surveillance projects of China that use Artificial Intelligence, new-age technology, sophisticated surveillance systems, and human intelligence. While many other projects are focused on cities and densely populated areas, Sharp Eyes focuses on rural areas. Its goal, according to the law enforcement agencies is mainly to assist the police in understaffed and remote places.

Sharp Eyes surveillance programme, according to reports, would mean more than 200 million public and private cameras being installed in public spaces to keep track of every activity which may not necessarily be a crime or even suspicious.[14]

RBI orders Mobikwik audit after data breach

In yet another incident of data breach just two months after the Juspay breach, a cyber-security researcher on March 29 claimed that user data that included sensitive information of 3.5 million Mobikwik (another payment company) users, were put up for sale on the dark web. The information contained the KYC details, addresses, phone numbers, Aadhar card details, etc. of Mobikwik users.

Soon after the incident, the payment app came under the scanner of the Reserve Bank of India (RBI). The RBI has asked the digital wallet firm to get a forensic audit done with the help of CERT-IN-(Indian Computer Emergency Response Team)-empanelled auditor, immediately.[15] The company for now is closely working with security authorities and has assured its users that their accounts and balances are completely safe. It has stated that the sensitive data is stored in encrypted form and any misuse is not possible without the one-time-password (OTP) that only comes on users' mobile number.

Several criticisms have been raised about the initial response of the company, and its threats of legal action against the information security researcher who brought the breach to its notice, rather than undertaking an investigation into the alleged breach.

UN OEWG on ICT developments submits report

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 in the context of international security and which is to submit its report in September 2021. The OEWG has built on the recommendations of the previous 5 UNGGEs on Developments in the Field of Information and Telecommunications in the Context of International Security in its report, thus reaffirming those recommendations since the OEWG is made up of all member states while the UNGGE has a much smaller membership.

The OEWG report had the following conclusions and recommendations: (A) Identifying Existing and Potential Threats- States experience varied levels of threats according to a State's levels of digitalization, capacity, ICT security and resilience, infrastructure and development and 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. (B)Rules, Norms and Principles for Responsible State Behaviour- 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 and the importance of supporting and furthering efforts to implement norms to which States have committed to be guided at the global, regional and national levels. (C) The OEWG recommends that States should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public. (D)Confidence-building measures (CBMs) - with the necessary resources, capacities and engagement, CBMs can strengthen the overall security, resilience and peaceful use of ICTs. CBMs can also support implementation of norms of responsible State behaviour, and can foster trust and ensure greater clarity, predictability and stability in the use of ICTs by States. (E) Regular Institutional Dialogue- States concluded that "regular institutional dialogue under the auspices of the United Nations should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results based."[16] 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. The current documentation of the OEWG outcomes also include a Chair's summary of discussions and recommendations that were not included in the final substantive report.[17]

Rules, norms and principles from India's written submissions by delegations (Extracts)

The submissions by India stated the importance of the OEWG procedure and recommendations of International law to ICT. It stated that cybersecurity and International security are matters of substantial importance. It proposed for new norms related to the need for an agreed standard of essential security in cyberspace on the most effective ways to optimize the promising technologies while safeguarding the public.

In cooperation with the observation of member states, it was concluded that the states shall strongly endorse the widespread adoption and verified implementation of basic cyber hygiene. Responsible behaviour of the States include protection of critical information infrastructure (CII) since any threat to CII can spoil integrity of information and damage the economic development of a nation.

Protection of CII can be done with the help of public-private partnership models. States should be responsible for notifying users when significant vulnerabilities are identified, and notifying vendors to patch those vulnerabilities. It is the role of States to work collaboratively on CII, through exchange of information on threats and sharing of mitigation tools and techniques.

[1] Ransomware attack on Pimpri Chinchwad Smart City servers at https://economictimes.indiatimes.com/tech/information-tech/ransomware-attack-on-pimpri-chinchwad-smart-city-servers-managed-by-tech-mahindra

[2] Cyber attack: Tech Mahindra in soup, PCMC not to pay damages at https://indianexpress.com/article/cities/pune/cyber-attack-tech-mahindra-in-soup-pcmc-not-to-pay-damages-parties-seek-thorough-probe-7227737/

[3]IBM X-Force Threat Intelligence Index at https://www.ibm.com/security/data-breach/threat-intelligence

[4] Cyber Attacks: India second-most attacked country in Asia Pacific region, says IBM Security at https://www.financialexpress.com/industry/technology/cyber-attacks-india-second-most-attacked-country-in-asia-pacific-region-says-ibm-security/2211702/

[5] India second in list of countries facing cyberattacks in Asia-Pacific in 2020: IBM Security Report at https://indianexpress.com/article/technology/tech-news-technology/india-second-asia-list-cyberattacks-ransomware-attacks-ibm-security-report-2020-7202785/

[6] At least 32 Indian companies have been attacked by cyber criminals at https://www.businessinsider.in/tech/news/at-least-32-indian-companies-have-been-attacked-by-cyber-criminals-using-microsofts-email-servers/articleshow/81511936.cms

[7]Charting a course towards a more privacy-first web at https://blog.google/products/ads-commerce/a-more-privacy-first-web/

[8]Google Chrome's privacy changes will hit the web later this year at https://www.cnet.com/news/google-chromes-privacy-changes-will-hit-the-web-later-this-year/

[9] Google will stop selling ads based on tracked individual browsing history at https://www.cnet.com/news/google-will-stop-selling-ads-based-on-tracked-individual-browsing-history/

[10] Google hit with its third antitrust lawsuit since October at https://www.cnbc.com/2020/12/17/google-faces-a-third-government-antitrust-lawsuit.html

[11] Grab partners with Indonesian government to open COVID drive-through vaccination centre at https://www.zdnet.com/article/grab-partners-with-indonesian-government-to-open-covid-drive-through-vaccination-centre/

[12] Grab Drive-Through Service to Boost Indonesia Vaccine Drive at https://www.bloombergquint.com/onweb/grab-drive-thru-service-to-boost-indonesia-vaccination-campaign

[13] China’s ‘Sharp Eyes’ Program Aims to Surveil 100% of Public Space at https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015

[14] Almost 100% of China’s public spaces under watch at https://www.opindia.com/2021/03/china-instrusive-surveillance-citizens-sharp-eyes-ccp-cctv/

[15]RBI orders forensic audit of Mobikwik systems after data breach allegations at https://www.livemint.com/companies/news/rbi-orders-forensic-audit-of-mobikwik-systems-after-data-breach-allegations-11617207623780.html

[16] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[17] https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf