MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE
Liberté
Égalité
Fraternité

Direction générale du Trésor

REVUE DE PRESSE SECTORIELLE NUMERIQUE

UNE PUBLICATION DU SERVICE ÉCONOMIQUE REGIONAL DE NEW DELHI

N° 2 – 1-19 Mars 2021

G En bref

TIC :

- La société Cyfirma, basée à Singapour, signale que des pirates informatiques s'en prennent aux données des essais du vaccin Covid19 du All India Institute of Medical Sciences, du Serum Institute of India, de Bharat Biotech et de Zydus Cadila.

- Une série de cyberattaques présumées va donner lieu à une nouvelle stratégie de cybersécurité coordonnant les ministères indiens de l'intérieur, des technologies de l'information, de la défense et le « National Critical Information Infrastructure Protection Center ».

- Une commission parlementaire s'interroge sur les nouvelles règles applicables aux plateformes de streaming (OTT) et aux réseaux sociaux

- Le *Department of Science & Technology*, le *Ministry of Electronics and Information Technology* et NITI Aayog mènent au moins 12 projets basés sur l'intelligence artificielle pour améliorer les services gouvernementaux.

TÉLÉCOMMUNICATIONS:

- L'Autorité de régulation des télécommunications de l'Inde (TRAI) suspend 7 jours la mise en œuvre de la réglementation relative aux spams. Plusieurs services en ligne ont signalé des perturbations dues à la non-conformité.

- À partir du 15 juin 2021, les fournisseurs de services internet indiens ne pourront utiliser que des équipements de télécommunication figurant sur une liste de produits dit « de confiance ».

- Capgemini ouvre deux laboratoires 5G à Paris et à Mumbai pour permettre à l'industrie d'expérimenter et de déployer les technologies 5G et celles connexes.

Revue de presse

1. TIC

China, Russia & North Korea hackers target AIIMS, SII, Patanjali for Covid data — report

The Print, 2/03/2021

New Delhi: A group of Chinese, Russian and North Korean hackers have targeted crucial information of India's top drug and vaccine makers including Serum Institute of India (SII), Bharat Biotech, Zydus Cadila and AIIMS, cyber intelligence firm Cyfirma has found.

Bharat Biotech and SII have developed vaccines against Covid-19 in India, which were approved for emergency use authorisation in the country in January, and Zydus Cadila is involved in the last stage trial of its Covid vaccine. The All India Institute of Medical Sciences (AIIMS) is the country's apex public hospital and research institute.

Cyfirma, which is backed by US financial firm Goldman Sachs and is based in Singapore and Tokyo, had noticed "eminent threats" to global healthcare companies by hackers between 24 to 26 February.

"The early warnings were identified where we noted the eminent threats related to the IT assets of the global healthcare companies including several Indian firms," Kumar Ritesh, chief executive officer of Cyfirma told ThePrint.

According to the firm's report, these cyberattacks originated from three major state-sponsored threat groups that were primarily based in Russia, China and North Korea.

The report, which was accessed by ThePrint, further noted that apart from India, healthcare companies in the US, UK, Japan, Australia, South Korea, Italy, Spain, Germany, Brazil, Taiwan and Mexico were also targeted.

"Researchers have observed the hacking groups are aiming to steal COVID-19 vaccine related data. This includes vaccine research, medical composition, clinical trials information, logistics and distribution plans," the report said.

It added that "there is a global competition among nations, and in parallel, there are heightened activities among cybercriminals who are motivated to seek competitive advantage for their countries".

The Print reached AIIMS, SII, Bharat Biotech, Zydus Cadila, Lupin and Sun Pharma via email for a comment but received no response till the time of publishing this report.

A source at SII said the firm was "strengthening" its IT assets but did not confirm or deny the attack.

Vaccine research, trial data draw attention

A key observation from the report highlighted that clinical trial data of vaccines has been of particular interest to these hackers.

"India's series of clinical trials involving millions of research records is highly valuable. This data can help accelerate research work in aid of producing more effective vaccines," noted the report, which was submitted to the Indian Computer Emergency Response Team (CERT) — the nodal agency under the Ministry of Electronics and Information Technology that deals with cyber threats.

The report further stated that hackers view India as an easy target as the country's cybersecurity maturity level is relatively low.

"Cyfirma recommends India CERT authorities to alert the targeted companies and take immediate measures to mitigate these attacks," it said.

"We have submitted the report but haven't heard back from CERT if they have forwarded the information to the companies concerned," said Ritesh, a former top cyber official with British intelligence agency MI6.

His team of researchers also noticed an increased interest in India's vaccine research and development by these state-sponsored threat actors.

"India was lagging in the COVID-19 vaccine research and started to catch up in the last couple of months. This has drawn the attention of Chinese state-sponsored threat actors whose intentions are to tarnish India's reputation as well as to disrupt her national vaccination effort," the report said.

It added: "Russian state-sponsored threat actors are seeking a combination of geopolitical gain as well as financial rewards while Korean threat groups are focused on financial gain."
North Korea attacks Patanjali, Chinese group targets SII, Bharat Biotech

The report contains details about cyber attack campaigns that are in the making and currently underway.

The Russian hacking group ATP 29, has either targeted or is looking to target 18 global pharmaceutical companies, hospitals, healthcare support, universities and research firms, and approving authorities.

These include Pfizer, Cipla, AstraZeneca, Divi's Labs, Dr. Reddy's, Abbott India, Torrent Pharma, Zydus Cadila and AIIMS.

Meanwhile, APT 10, the Chinese group, has identified 17 global organisations including Sun pharma, Ahmedabad Civil Hospital, Lupin, SII, Bharat Biotech and AIIMS.

The North Korean group has identified 14 global organisations including Dr. Reddy's, Torrent Pharma, SII and Patanjali.

"These groups are either looking at committing cyber crimes at these firms or have already started doing (so)," Ritesh said.
What else is being targeted?

The Cyfirma researchers have observed 15 active hacking campaigns — seven Russian groups, four Chinese, three Korean and one from Iran.

According to them, these hackers are targeting multiple assets of pharmaceutical companies who are investing in medical research, clinical trials and vaccine production.

They also target the vaccine supply chains, national vaccination campaigns, individual and personal information apart from government agencies in charge of approving vaccines, medicines and related appliances.

Vaccine development and implementation tracking systems, clinical trial information, hospital operating details, employee and patient information are also being targeted.

The report noted that the objective of the hackers is to secure sensitive information related to vaccines and medical research for competitive advantage.

The other objectives include exfiltrate vaccine trial information, intellectual property theft, financial gain, business advantage and reputation damage to competition.

India plans new cybersecurity strategy after 'Chinese intrusions'

Bloomberg, 9/03/2021

New Delhi: India is mulling a new national strategy to strengthen the country's cybersecurity amid allegations that Chinese intrusions may have affected operations at a key stock exchange and supply of electricity in the country's commercial capital.

The plan will coordinate responses across ministries including Home Affairs, Information Technology, Defense and the National Critical Information Infrastructure Protection Centre in case of an attack and set audit procedures, former Lieutenant General Rajesh Pant, India's National Cyber Security Coordinator said in an interview. It will be approved by the cabinet committee on security headed by Prime Minister Narendra Modi.

Authorities are investigating a series of recent suspected cyber intrusions which could have led to a power outage in Mumbai, crippled systems at banks and caused a glitch at the country's premier National Stock Exchange, he said. A report is expected in about a fortnight.

"We also want to know what happened," said Pant, who served in the Indian army and now coordinates India's cyber intelligence and reports to the Prime Minister's Office. He said the breaches were likely malware and couldn't be classified as attacks without a proper investigation.

At least one connection opened by Chinese state-sponsored hackers into the network system of an Indian port was still active, as authorities blocked attempts to penetrate the South Asian nation's electrical sector, the U.S.-based research firm Recorded Future said last week. The attempts by the Red Echo group have been occurring since at least the middle of last year, around the time a bloody skirmish between Indian and Chinese soldiers started in the remote Himalayan region, the firm said.

"India will have to work at breakneck speed to put in place stringent security for critical infrastructure," said Sandeep Shukla, who runs a state-funded cybersecurity project at the Indian Institute of Technology, Kanpur, and has advised the federal government in the past. "There may also be a need for state financial backing to help smaller companies that are part of the grid. Because if one is hacked, entire systems can be compromised."

The new strategy will lay down protocols for prevention and audit to secure the government's digitally connected water, health and education systems that are all being treated as critical infrastructure, he said. Infrastructure like nuclear, power and aviation will be considered supercritical.

"In my view, if internet-connected computers are infected by malware, I won't say it's an attack but an infection unless it jumps from IT systems to other operation systems," Pant said. "It's like a crank caller. Can you stop someone from dialing your number?"

Parliamentary panel members question legality of new rules for OTT, social media platforms

Press Trust of India, 16/03/2021

Some members of the Parliamentary Standing Committee on Information Technology on Monday questioned the legality of new rules framed by the government to regulate OTT and social media platforms. Tightening the rules governing social media and streaming companies, the Centre had announced last month the Intermediary Guidelines and Digital Media Ethics Code applicable on WhatsApp, Facebook, Twitter, Netflix, YouTube and Amazon Prime Video among others.

Top officials of the Information and Broadcasting Ministry and the Ministry of Electronics and Information Technology on Monday deposed before the parliamentary panel on "intermediary guidelines in the context of examination of the subject review of functioning of Central Board of Film Certification."

The panel is chaired by senior Congress leader Shashi Tharoor.

Some members and the chairman asked a number of questions to the officials like whether these rules are in conformity with the legal framework, sources in the panel said.

MPs from different parties in the panel also grilled the officials as to why the regulatory mechanism consists of only bureaucrats and not representatives of civil society, judiciary and professionals, they said.

According to sources, members also asked the officials whether they had consulted stakeholders before bringing these rules.

Briefing the members of the panel, government officials justified the need for such rules in changing times and also explained the rationale behind them.

The new rules or guidelines require social media and streaming platforms to take down contentious content quickly, appoint grievance redressal officers and assist investigations.

Beyond streaming and messaging platforms, the new rules also set code for digital publishers of news and current affairs content, requiring them to disclose their ownership and other information.

Union IT and Communications Minister Ravi Shankar Prasad had said that the guidelines for intermediaries and ethics code for digital media are designed to curb misuse of social media platforms as well as streaming services and disclose the first originator of the mischievous information and remove, within 24 hours, content depicting nudity or morphed pictures of women.

Prosthetic hands, detecting low birth weight in babies: The many govt AI projects in the works

The Print, 17/03/2021

New Delhi: The Department of Science & Technology (DST), IT ministry and Niti Aayog are testing out how artificial intelligence (AI) can be used in the services provided to people.

The government’s efforts were highlighted in a 16 March response to an unstarred question in Rajya Sabha asked by Trinamool Congress MP from West Bengal Manas Ranjan Bhunia.

Bhunia had asked if there was research being done by the government in the field of AI, especially relating to provision of government services, and the details of such efforts.

In response, Dr Harsh Vardhan, Union minister in charge of health, science and technology, and earth science ministries shared details of the government’s research.

DST

The Department of Science & Technology has set up a Technology Innovation Hub (TIH) on AI at the Indian Institute of Technology (IIT) in Kharagpur. The objective is to conduct research, translation and technology development, especially in how to provide government services, the minister said.

IT ministry

There are eight IT ministry initiatives for researching AI applications in government services.

These include automated speech recognition in English, Hindi, Tamil. Text-to-speech synthesis for conversational speech in Indian languages is also being researched.

Indian language to Indian language translation using AI is also being tested.

The ministry is also developing an ‘English-Marathi-English Machine Translation System’.

The initiatives also research into a Bilingual Optical Character Recognition. Optical Character Recognition means the electronic scanning and identification of handwritten or printed text, and its subsequent conversion into text can be edited by a computer according to Collins dictionary.

The IT ministry is also researching sensor-based prosthetic hands, pesticide and fertiliser spray system using drones, and an AI-based recommendation engine for the government’s e-marketplace.

Dr Harsh Vardhan’s response also mentioned that under the IT ministry’s Visvesvaraya PhD Scheme, over 80 research scholars are conducting research on AI and related fields.

Niti Aayog

Niti Aayog has three pilot projects in the works that use AI to provide government services.

These include a “Clinical Decision Support System Project in the aspirational district of Bahraich”, according to the minister’s response. The system aims to get frontline health workers to use digital methods to issue advisories to pregnant mothers and children, and to avoid the use of “physical registries which can be error prone and time consuming”.

The AI-based system also aims to allow these health workers to move away from being just “mere agents of implementation into intermediate care-givers”.

Another Niti Aayog pilot is an AI-enabled Diabetic Retinopathy Detection System using retinal scans. The pilot is being conducted in the district of Moga and in Mohali. Automating retinopathy detection will lessen burden on health systems and ophthalmologists as it can be used for mass screening in under-served areas, the government’s response noted.

Retinopathy is when the retina part of the eye is damaged.

In addition, Niti Aayog is testing out smartphone solutions to detect low birth weight in babies. The pilot project is being conducted in the districts of Baran in Rajasthan and Balrampur in Uttar Pradesh.

2. Télécommunications

Telcos told to switch off SMS filter for 7 Days

ET Telecom, 10/03/2021

New Delhi:

The Telecom Regulatory Authority of India (Trai) on Tuesday suspended the implementation of its regulation to control pesky messages for a week, a day after a host of services and transactions such as net banking, online railway ticket bookings, ecommerce sales and Aadhaar authentication were disrupted as SMSes and OTPs failed to arrive.

“It has been observed that some of the principal entities have not fulfilled the requirements as envisaged in Telecom Commercial

Communications Customer Preference Regulations, 2018 (TCCCPR, 2018)," Trai said in a statement, adding that this was resulting in SMSes getting dropped. The regulator added that it had suspended the implementation of the regulation for seven days, to ensure no inconvenience is caused to customers.

ET had, in its March 9 edition, reported about the disruption caused to several online services because of the inability of telemarketers and others to register their sender IDs and context of texts on the blockchain platform of telcos.

'Smaller Players Struggling to Catch Up'

This resulted in a large number of bulk text messages not going through.

According to sources aware of the matter, the overall commercial SMS drop rate came down to 33% on Tuesday from 40% the day before. For banking and financial services, the failure rate on Tuesday was 10% against 25% on Monday. On average, over 1 billion commercial SMSes are sent per day in India.

Telecom executives say they have received instructions from Trai and are switching off the filtration process today (Tuesday) itself. Leading telemarketers such as Kaleyra and Tanla-owned Karix said the relaxation will give time to companies who have ignored reminders in the past.

Industry executives said that though larger brands and telemarketers with advanced IT mechanisms in place are gradually catching up to the rigid blockchain filters, the smaller market players are struggling to so as SMS content is dynamic.

According to Trai's regulations on unsolicited commercial communication, which were issued in 2018 but implemented fully starting Monday, telcos must verify every SMS content with a registered text before delivering it. The blockchain-based solution deployed by telecom operators checks the sender id, called the header, and content of every commercial SMS originating from a registered source.

SMSes from unregistered sender ids are simply blocked. In fact, the system automatically filters SMSes with even a small change such as the addition and deletion of a full stop.

Speaking to ET, a senior Trai official denied that any large disruption had taken place, and called out enterprises for failure to register their SMS content by the March 8, 2020 deadline, despite several newspaper ads and repeated reminders sent out by telcos.

"We will have to switch off the process of filtration as directed. However, the principal entities (enterprises) will now have to register within one week after which there should not be any problem again," said a senior executive at one of the three private telcos.

Another telco executive added that a week's deadline is enough for all entities to register, and no one can blame the operators for any OTP misses.

DoT amends ISP licenses on telecom gear use from trusted sources, products lists

ET Telecom, 16/03/2021

The Department of Telecommunications (DoT) has brought in the clause of "trusted sources" and "trusted products" while amending the licenses of internet service providers (ISPs) for providing telecom gear.

According to the new directive, from June 15, companies like state-run GAIL, RailTel, Power Grid, Oil India which have ISP licenses can only install equipment from the trusted products list.

"The government through the designated authority will have the right to impose conditions for procurement of telecommunication equipment on grounds of Defense of India, or

matters directly or indirectly related thereto, for national security. Designated authority for this purpose shall be National Cybersecurity Coordinator. In this regard, the licensee shall provide any information as and when sought by the Designated Authority," said DoT on Tuesday.

" With effect from 15 June 2021. the licensee shall only connect Trusted Products in its network, and also seek permission from designated authority for upgradation of existing network utilizing the Telecommunication Equipment, not designated as Trusted Products," it added.

However, these directions will not affect ongoing annual maintenance contracts or updates to existing equipment already inducted in the network, as on date of effect.

The department had earlier similarly amended telecom licenses

Since the outbreak of the latest Sino-Indian border tensions earlier this year,the government has taken a series of steps to make it tougher for Chinese companies to operate in India.

It has stipulated that companies belonging to countries sharing a border with India can no longer invest under the automatic route and need their investments to be vetted by the Indian authorities. In addition, around 220 Chinese apps, including popular ones such as TikTok, have been banned for national security reasons.

New Delhi has also been unofficially nudging private and state-run telcos to start avoiding Chinese equipment, but Wednesday's is the first official step in the direction of barring their involvement in Indian networks,especially the5G rollout.

This, even as the geopolitical tensions have reached a point of stalemate with both sides amassing thousands of troops and digging in at the borders even in harsh winter conditions. Telcos had been pushing the government to take a clear stance on Chinese vendors, which would enable them to take future investment decisions.

Global consultancy, CapGemini opens 5G labs in Paris and Mumbai

SmartCitiesWorld, 17/03/2021

Consulting, digital transformation, technology and engineering services firm Capgemini has opened two 5G labs in Paris and Mumbai to enable industry experimentation and deployment of 5G- and edge technologies.

Each of the labs bid to help organisations across every industry to 'pivot' their business to be ready to take advantage of the 5G and edge revolution.

Network capabilities

According to Capgemini, they also complement the 5G lab for telecommunications companies, enterprises and original equipment manufacturers (OEMs) which opened in December 2020 in Portugal, focused on the development of network capabilities and solutions.

The multidisciplinary team of experts at the labs will accompany organisations in the exploration of the latest use cases; experiencing new perspectives on how 5G is transforming their industry; and in helping them to build, monetise, and strategise what 5G brings next for their business. Services include strategy, ideation and planning, use case design and development, and ecosystem orchestration and integration.

The labs will draw on an innovation ecosystem of partners to experience all the new possibilities offered to organisations and help build their end-to-end solutions. Capgemini claims they integrate the latest networking, cloud- and edge computing technologies with cutting-edge 5G connectivity, and an agile and modular application environment.

With an ecosystem of partners (both telecom and technology driven) and focus on end-to-end solutions for industries, Capgemini's 5G experts have developed four dedicated areas of specialty, based on industry requirements and proven use cases:

Smart cities: for the public sector (including transport, health, education); it covers services provided to large samples of population. Examples of use cases: public transport infotainment; immersive learning; crowd management; and telemedicine

Smart utilities: for the energy and chemicals sectors; it covers processes, logistics and operations. Examples of use cases: remote monitoring of sites; mission-critical process control; energy efficiency; and sustainability

Smart factory: for the manufacturing and automotive sector; it covers production activities carried out in factories and warehouses. Examples of use cases: augmented remote assistance; autonomous devices in warehouse and assembly lines; computer vision based quality assurance; and safety and surveillance

Smart retail: for the retail, consumer goods and luxury goods sector; it covers activities that enhance the personalisation of services to end consumers. Examples of use cases: immersive shopping experience; and purchase automation via smart carts.

"5G brings a step-change in connectivity and automation to all industries and opens new perspectives and possibilities for business. "By embracing the 5G digital revolution, organisations will be able to take advantage of the increasing volume of data and derive real-time actionable insights," said Pierre Fortier, head of 5G at Capgemini Invent.

"Our 5G labs in Paris and Mumbai are designed to accompany organisations in their transformation journey towards Intelligent Industry, onboarding them in the 5G ecosystem to explore all innovation possibilities and helping them to build and monetise customised end-to end solutions for their business."

La direction générale du Trésor est présente dans plus de 100 pays à travers ses Services économiques.
Pour en savoir plus sur ses missions et ses implantations : **www.tresor.economie.gouv.fr/tresor-international**

MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE
Liberté
Égalité
Fraternité

Responsable de la publication : **Service économique de New Delhi**
Rédacteurs : **Feli VISCO**

Pour s'abonner : Contacter le SER de New Delhi
Crédits photo : **©DG Trésor**