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

CYBER *Digest*

August 2021

- **US and allies condemn China for Microsoft hack**
- **Ransomware attack on Kaseya**
- **French antitrust watchdog fines Google €500m**
- **Malaysia chooses Ericsson over Huawei for its 5G network**
- **Israel launches commission to probe Pegasus spyware**
- **Chinese authorities order Didi off app stores**
- **Transnet restores operations at ports post cyber attack**

US and allies condemn China for Microsoft hack

On July 19, the United States Department of Justice (DoJ) accused four Chinese nationals of hacking into the popular email platform, Microsoft Exchange. The Chinese nationals were charged with hacking, extortion and threatening the national security. The hack, disclosed by Microsoft earlier in March affected at least 30,000 organisations that included government as well as private entities both in the US and worldwide.

Microsoft accused the Chinese cyberespionage group, Hafnium, for targeting Microsoft Exchange systems, through a vulnerability in the software which gave hackers access the mail inboxes.[1]

Apart from the United States, the European Union, NATO and other world powers also accused the Chinese government of the Microsoft attack and other malicious cyber activities.[2] China however has denied all such allegations, calling them fabricated. The escalation in the intensity and frequency of such attacks, and the near-absence of an international response do not augur well for the continuing security and stability of cyberspace.

Ransomware attack on Kaseya

The ransomware attack that took place on July 2 targeting thousands of organisations using the Kaseya IT management software, was finally fixed after obtaining a decryptor from a third party, according to the the IT firm. The REvil gang, a cybercriminal group took credit for the massive international ransomware outbreak, charged a ransom of $70 million and claimed to have locked down millions of devices.

In a further twist, dark web sites linked to the "REvil ransomware gang" stopped operating with the message "a server with the specified hostname could not be found" on July 13th. The REvil gang also reportedly left the online forums through which they used to communicate with the victims of the attack.

Kaseya stated on July 21 that it has obtained a universal decryptor for restoration of the encrypted data from Emsisoft, a cybersecurity firm. Kaseya is now working to remediate its customers who were impacted by the attack. But Kaseya has not confirmed whether it has paid the ransom amount or not. There is strong speculation that the decryptor key was obtained as a results of the efforts of either the US government, the Russian government, or because a ransom was in fact paid to the cybercriminals.

French antitrust watchdog fines Google €500m

A French antitrust watchdog has fined Google €500m for noncompliance with its orders on conducting talks with the news publishers in the country on a copyright row. According to the antitrust authority, Google breached orders which demanded that such talks should take place within three months of any news publisher asking for it.[3]

The agreement, a deal under Google's News Showcase programme, is the first of its kind in Europe which mandates Google to provide compensation for news snippets used in its search results. In order to end the copyright row, Google has also agreed to pay $76m to a group of French news publishers.

The antitrust watchdog has also accused Google of not acting in "good faith" in its negotiations with the publishers and asked it to come up with proposals on how it would compensate the news agencies for the use of their news within the next two months,failing which the company might have to face

additional fines of up to €900,000 per day.

Google stated that it was very disappointed to face the accusation since the fine ignores the efforts to reach an agreement and provide an explanation regarding the reality of how news works on its platforms, but would however comply with it.

Malaysia chooses Ericsson over Huawei for its 5G network

The Malaysian government has handed over the contract to build its 5G telecommunications network to the Ericsson of Sweden for 11 billion ringgit which is approximately $2.6 billion. Ericsson as per the contract will handle the design and development of end-to-end 5G network in the country.[4]

Malaysia aims to make 5G connectivity available in the country by the end of 2021 and to reach a target of 80% of the population by 2024. In the initial phase, services will be rolled out in Kuala Lumpur, Putrajaya, the federal capital, and Cyberjaya, the multimedia hub.

As per reports, eight vendors had participated in the tender including Huawei, ZTE, Cisco, NEC, Nokia, Samsung and FiberHome, out of which Ericsson was chosen. Ericsson also plans value-creation activities worth 4 billion ringgit in the country via knowledge building and technology transfer plans throughout the tenure of the contract.

The move by Malaysia to hand over the 5G contract to Ericsson over Hauwei however does not indicate any strong aversion towards it because Malaysia is already in a partnership with Huawei on a cybersecurity lab since February 2021.

Ericsson would collaborate with *Digital Nasional*, a Special Purpose Vehicle owned by the Ministry of Finance (MOF) for faster connectivity speeds and greater bandwidth of 5G for mobile broadband. The deal will also benefit local contractors over the next 10 years.

Israel launches commission to probe Pegasus spyware

The head of the Israeli parliament's Foreign Affairs and Defence Committee announced on July 22 that a commission has been established to review the allegations on the Israel-based firm NSO, the developer of the Pegasus spyware.[5]

The firm was accused of selling spyware technology to various customers worldwide that was misused for mass surveillance on activists and journalists, heads of states, and many others through their spyware Pegasus. A list of 50,000 potential targets was leaked to Amnesty International, the rights group and Paris-based Forbidden Stories. NSO however has denied these allegations stating that the leak is "not a list of targets or potential targets of Pegasus."

The Pegasus spyware is capable of hacking mobile phones without even the knowledge of the victim and in turn can extract vital information like messages, user's location, and can also be used to gain access to the phone's camera and the microphone.

The revelations sparked off a heated debate worldwide on accountability and human rights. The committee would look into the prospect of tighter controls on the export of spyware such as Pegasus and licenses granted by Defence Exports Control Agency of Israel.

Chinese authorities order Didi off app stores

The Cyberspace Administration of China (CAC) ordered smartphone app stores to remove Didi, the ride hailing app off their stores, after accusations of it collecting personal user data illegally.[6]

CAC had asked Didi to make changes in its policy so as to comply with Chinese data protection rules in a statement on its social media feed. CAC also announced an investigation into Didi to protect "national security and the public interest" although it had not specified the nature of violation of rules by the app. In response, Didi stated that it has stopped registering new users and would remove the app from respective app stores and would make the necessary changes to comply with rules and rights of users. Didi's app was however still working for people in China who had already downloaded it.

Didi, which offers over 20 million rides in China per day and many other markets, is known to collect vast amounts data on real-time mobility every day. Some of this data is also used for autonomous driving technologies and traffic analysis. Didi was also previously subjected to a regulatory probe on its operating license. The clampdown on Didi is the latest in a series of actions against big tech operators by the Chinese government citing privacy and sector dominance and abuse concerns.

Transnet restores operations at ports post cyber attack

South African state logistics firm Transnet that became the victim of a cyber-attack on July 22, restored its operations after several days, on July 29 at the major ports that it operates.[7] Transnet, a government owned logistics firm, operates major South African ports and freight railway networks in the country.

The attack affected container terminals at key ports of Durban, Ngqura, Port Elizabeth and Cape Town. It forced Transnet to switch to the manual functioning of their systems impacting exports and imports in the country. Transnet, following the disruptions declared "force majeure" - a clause preventing it from fulfilling its contract due to unforeseen circumstances.

According to Ministry of Public Enterprises of South Africa, customer data from Transnet had not been compromised by the cyber-attack. On July 29, it declared that the Durban's container terminals were restored and container operations in the Eastern Cape were in the process of restoration. Transnet meanwhile stated that the force majeure was being reviewed and would be lifted by August 2, once the IT systems become fully functional.

---

[1] China accused of cyber-attack on Microsoft Exchange servers at

https://www.bbc.com/news/world-asia-china-57889981

[2] U.S., allies accuse China of hacking Microsoft and condoning other cyberattacks at

https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html

[3] Google fined €500m by France's antitrust watchdog over copyright at

https://www.theguardian.com/technology/2021/jul/13/google-fined-500m-by-frances-antitrust-watchdog-over-copyright

[4] Malaysia picks Ericsson over Huawei to build 5G network at

https://asia.nikkei.com/Spotlight/5G-networks/Malaysia-picks-Ericsson-over-Huawei-to-build-5G-network

[5]Israel launches commission to probe Pegasus spyware: Legislator at

https://www.aljazeera.com/news/2021/7/22/israel-launches-commission-to-probe-pegasus-spyware-legislator

[6] China's cyberspace regulator orders Didi off app stores after launching investigation at

https://www.abc.net.au/news/2021-07-05/didi-ordered-off-app-stores/100267228

[7] South Africa's Transnet restores operations at ports after cyber attack at

https://www.reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ