

## From Page One

### Foxconn signs deal with T.N. to build plant in Kancheepuram

Later in the day, Mr. Liu signed a tripartite Memorandum of Understanding (MoU) with Indian Institute of Technology - Madras (IIT-M) and Guidance (the nodal agency instrumental in bringing investments to the State).

According to a senior government official, the MoU enables Foxconn to support research and development capabilities in partnership with IIT-M for Tamil Nadu to improve the talent pool's skills and industry readiness to cater to the evolving needs of the electronics industry and share knowledge and best practices in higher-order talent and workforce development.

Mr. Liu also went to IIT-M Research Park with State Minister for Industries, Investment Promotion and Commerce T.R.B. Rajaa and his team. The duo held discussions with Ashok Jhunjhunwala, president of IIT-M Research Park and IIT-M Incubation cell.

After visiting a few start-ups inside the research park, Mr. Liu, in a quick interaction with media, said he also visited the company's largest plant in India at Sriperumbudur, which employs about 40,000 people. "There are six to seven buildings that are under construction at the facility. It is going quite well, and we can definitely do more in the future," he added.

Mr. Rajaa said: "Foxconn's repeated investments and expansion plans in Tamil Nadu are a testament to the State being the top choice for manufacturing in India for major companies across the world," and added, "With this proposed investment, and many more to come, Tamil Nadu is poised to not only remain the top electronics exporter in the country but also significantly increase its electronics exports in the coming years. This will play a critical role in attaining our Chief Minister's ambition of a \$1-trillion economy in Tamil Nadu."

## Foxconn signs deal with T.N. to build plant in Kancheepuram

**Sangeetha Kandavel**  
CHENNAI

Taiwanese firm Foxconn Technology Group, a key supplier to Apple Inc., on Monday gave a commitment to the Tamil Nadu government to invest ₹1,600 crore to establish a manufacturing facility in Kancheepuram district.

The investment will be made by its subsidiary Foxconn Industrial Internet (Fii).

A letter of intent was signed in the presence of Chief Minister M.K. Stalin and Foxconn Chairman Young Liu. This was also Mr. Liu's first visit to Tamil Nadu.



Foxconn Group Chairman Young Liu meeting Chief Minister M.K. Stalin in Chennai on Monday. SPECIAL ARRANGEMENT

"Was delighted to meet the Foxconn Group Chairman Mr. Young Liu and his team. Various investment opportunities in Tamil Nadu were discussed. Investment commitment to establish a mobile component manufacturing facility in Kancheepuram district for ₹1,600 crore, with a potential employment for 6,000

persons, was signed in my presence. Another milestone in our ambition to make Tamil Nadu the new emerging electronics manufacturing hub of Asia!" Mr. Stalin posted on the social media platform X (formerly Twitter).

**CONTINUED ON**  
» PAGE 2

**EVA STALIN IAS ACADEMY - BEST IAS COACHING IN CHENNAI**

**12/24, Muthurangan Muthali St, West Tambaram, Chennai - 600045**

<https://www.evastaliniasacademy.in/>

**Contact Number - +91-8678969915, +91-9940332851**

## Tamilians for Tamil Nadu project launched to skill 1,000 children from government schools

**The Hindu Bureau**  
CHENNAI

Tamilians for Tamil Nadu, a project to enable 1,000 children from government schools gain creative problem-solving skills through specially-curated projects and collaborate with eminent professors across the world, was launched in the city on Monday.

The students will receive scholarships to access projects in STEM (Science, Technology, Engineering and Mathematics) and humanities to nurture skills to solve real-world issues and will be guided in Tamil by professors across the world through the platform. This will lead to internship opportunities. The scheme has been introduced by Kruu, a project-based learning initiative founded by renowned pianist and educator Anil Srinivasan.

Launching the project at an event hosted jointly by Rhapsody Music Foundation and Kruu, School Education Minister Anbil Mahesh Poyyamozhi said it would empower children in government schools and expose them to critical thinking and skills to resolve real-world issues through project-based learning.

He lauded Kruu's initiative



Schoolchildren explaining their models at the launch of the Tamilians for Tamil Nadu, an initiative of Kruu, in Chennai on Monday. S.R. RAGHUNATHAN

to provide a platform for middle and high school students to learn and collaborate with professors and mentors across the world. On Kruu, Mr. Srinivasan said it was launched in 2022 and has reached out to nearly 2.55 lakh schoolchildren.

The students get to work in groups on curated projects, interact with best minds in the educational field and gain ex-

pertise. Kruu aims to foster entrepreneurship and empower students to be creative thinkers, he said.

Earlier, student teams from various city schools presented their projects based on IoT and machine learning for solving issues like better access to healthcare facilities, senior citizens mobility and mobile applications for children with autism.

**EVA STALIN IAS ACADEMY - BEST IAS COACHING IN CHENNAI**

**12/24, Muthurangan Muthali St, West Tambaram, Chennai - 600045**

<https://www.evastaliniasacademy.in/>

**Contact Number - +91-8678969915, +91-9940332851**

## Chip tactics

The pitch to draw in semiconductor players must go beyond incentives

**T**he government has made a fresh bid to attract major global chip manufacturers into the country. At the Semicon India summit last Friday, Prime Minister Narendra Modi told prospective investors that the government had drawn on their suggestions after the first such conference last year, and taken pro-active decisions to address areas of concern. Apart from low corporate tax rates and sops for all new manufacturing projects, he said the incentives offered to tech firms to set up production facilities under India's semiconductor programme have been scaled up to 50% financial assistance. So, essentially, the government would bear half of the typically large investment outlays that companies commit to undertake. Ahead of Mr. Modi's U.S. State visit, the decks were cleared for a \$2.75 billion assembly, testing, marking and packaging facility in Gujarat proposed by the U.S.-based Micron Technology. The deal, perhaps nudged by the two countries' cooperation pact to build a semiconductors supply chain, has piqued investor interest and spurred Micron's suppliers to explore the option of co-located facilities.

With several countries seeking to de-risk themselves from the dominance of China in the chips manufacturing supply-chain through collaborative or 'friendshoring' arrangements, the rationale for the enhanced pitch to investors is unquestionable. But the competition is already fierce. The \$52 billion financing support announced by the U.S. for semiconductor makers in 2021 has drawn over \$200 billion in commitments. Wooed by an array of subsidies, Intel alone has committed \$80 billion in outlays across the European Union. In India, a \$10 billion production-linked incentive scheme was unveiled for chip makers in late 2021. A \$20 billion venture announced by Vedanta and Foxconn last year has, however, come undone. It is critical that the Micron investment is hand-held till fruition to create an effective exemplar effect. Apart from incentives, investors also need to see evidence of a stable operating environment with a predictable policy framework that is not amenable to knee-jerk deviations such as export curbs to cope with shortages. They would also compare India's trade linkages with world markets through bilateral or multilateral compacts and its approach to tariffs on myriad components that may need to be shipped in. The Prime Minister's assurance of understanding the needs of the global chip supply chain needs to be matched by actions to assuage such concerns. There could still be many a slip between the lip and the chip.

## ISRO successfully puts Chandrayaan-3 in translunar orbit

**Hemanth C.S.**  
BENGALURU

The Indian Space Research Organisation (ISRO) performed the TransLunar Injection (TLI) to slingshot Chandrayaan-3 towards the moon early on Tuesday. The TLI was performed successfully from ISRO Telemetry, Tracking and Command Network (ISTRAC) in Bengaluru.

"Chandrayaan-3 completes its orbits around the Earth and heads towards the Moon. A successful perigee-firing performed at ISTRAC, ISRO has injected the spacecraft into the translunar orbit," the space agency said. The TLI was planned for August 1 (Tuesday) between midnight and 1 a.m.

Chandrayaan-3 is expected to reach the lunar orbit on August 5 and the spacecraft's liquid engine will be fired again to insert the spacecraft into a lunar orbit. "The Lunar-Orbit Insertion (LOI) is planned for



ISRO's LVM-3 rocket lifts off with Chandrayaan-3 on board.

August 5," ISRO added.

After this, there will be four orbit manoeuvres to make the spacecraft enter into its final orbit at a distance of about 100 km from the moon's surface.

The Chandrayaan-3 consists of a lander module (LM), a propulsion module (PM) and a rover.

The PM and LM separation would happen on August 17. A series of deboost manoeuvres is also scheduled to take place before the power descent phase for soft-landing on the moon. The lander is expected to touch down on the moon surface on August 23 at 5.47 p.m.



## El Nino effect will suppress rainfall in the second half of the monsoon, says IMD

**The Hindu Bureau**  
NEW DELHI

After the torrential rain in July, August – usually the second rainiest of the four monsoon months – is likely to see “below normal” rainfall, the India Meteorological Department (IMD) said on Monday.

A strengthening El Nino and the absence of meteorological conditions that could have offset El Nino's effects will combine to suppress rainfall in the second half of the monsoon, IMD officials told *The Hindu*. Usually, August gets an average 25.49 cm of rainfall.

“The rainfall averaged over the country as a whole during second half of the monsoon season [August – September] is most likely to be normal [94-106% of the long period average (LPA)], with a tendency to be on negative side of the normal... The rainfall averaged over the country as a whole during August, 2023 is very likely to be below normal (<94% of LPA),” the IMD noted.

The LPA refers to a 50-year average.

On June 30, the IMD forecast that the July rainfall



**Rainstorm:** Commuters waded through a waterlogged road during heavy rain in Mumbai on Thursday. PTI

would be on the “positive side of normal” or at the most, 6% of what is usual for the month. However, a series of “western disturbances” (rain accentuating systems from Central Asia) and active monsoon conditions saw July receive nearly 13% more rainfall than what is typical for the month.

### Breaking records

Northwest India, overall, got the highest rainfall it has ever received since 2001 with Chandigarh, several parts of Haryana and Himachal Pradesh “breaking all-time records”, the IMD said.

Before the monsoon started in June, the IMD forecast rainfall for June-Sep-

tember to be 4% below normal. So far rainfall is 5% above what is usual for June and July combined.

“After the first week of August, we will see a drying up of rainfall in most parts of India and monsoon activity will shift to the northeastern States, eastern India and Himalayan foothill States,” D.S. Pai, senior meteorologist, IMD, told *The Hindu*. July usually gets 28 cm of rainfall.

Temperatures too are going to rise in August with “above normal” temperatures over most part of the south peninsula, east and northeast India and some parts of northwest and central India, the IMD said in a statement.

# Akira ransomware: why has the government issued a warning against it?

The government has issued a serious warning, urging users and corporations to implement robust cybersecurity measures to protect against this ransomware's double extortion tactics and potential data leaks

Nabeel Ahmed

**T**he Computer Emergency Response Team of India issued an alert for the ransomware dubbed "Akira." The ransomware, found to target both Windows and Linux devices, steals and encrypts data, forcing victims to pay double ransom for decryption and recovery.

The group behind the ransomware has already targeted multiple victims, mainly those located in the U.S., and has an active Akira ransomware leak site with information, including their most recent data leaks.

## What is the Akira ransomware?

The Akira ransomware is designed to encrypt data, create a ransomware note and delete Windows Shadow Volume copies on affected devices. The ransomware gets its name due to its ability to modify filenames of all encrypted files by appending them with the ".akira" extension.

The ransomware is designed to close processes or shut down Windows services that may keep it from encrypting files on the affected system.

It uses VPN services, especially when users have not enabled two-factor authentication, to trick users into downloading malicious files.

Once the ransomware infects a device

and steals/encrypts sensitive data, the group behind the attack extorts the victims into paying a ransom, threatening to release the data on their dark web blog if their demands are not met.

As mentioned above, the ransomware deletes the Windows Shadow Volume copies on the affected device. These files are instrumental in ensuring that organisations can back up data used in their applications for day-to-day functioning.

VSS services facilitate communication between different components without the need to take them offline, thereby ensuring data is backed up while it is also available for other functions.

Once the ransomware deletes the VSS files it proceeds to encrypt files with the pre-defined the ".akira" extension.

## How does Akira ransomware work?

The ransomware also terminates active Windows services using the Windows Restart Manager API, preventing any interference with the encryption process.

It is designed to not encrypt Program Data, Recycle Bin, Boot, System Volume information, and other folders instrumental in system stability. It also avoids modifying Windows system files with extensions like .syn, .msl and .exe. Once sensitive data is stolen and encrypted, the ransomware leaves behind a note named akira\_readme.txt which includes information about the attack and

the link to Akira's leak and negotiation site. Each victim is given a unique negotiation password to be entered into the threat actor's Tor site.

Unlike other ransomware operations, this negotiation site just includes a chat system that the victim can use to communicate with the ransomware gang, a report from The Bleeping Computer shares.

## How does ransomware infect devices?

Ransomware is typically spread through spear phishing emails that contain malicious attachments in the form of archived content (zip/rar) files. Other methods used to infect devices include drive-by-download, a cyber-attack that unintentionally downloads malicious code onto a device, and specially crafted web links in emails, clicking on which downloads malicious code.

The ransomware reportedly also spreads through insecure Remote Desktop connections.

In use since March 2023, the ransomware has steadily built up a list of victims, targeting corporate networks in various domains including education, finance, real estate, manufacturing, and consulting. Once it breaches a corporate network, the ransomware spreads laterally to other devices after gaining Windows domain admin credentials.

The threat actors also steal sensitive

corporate data for leverage in their extortion attempts.

## What can users do to protect against ransomware?

CERT-In has advised users to follow basic internet hygiene and protection protocols to ensure their security against ransomware. These include maintaining up to date offline backups of critical data, to prevent data loss in the event of an attack.

Additionally, users are advised to ensure all operating systems and networks are updated regularly, with virtual patching for legacy systems and networks.

Companies must also establish Domain-based Message Authentication, Reporting, and Conformance, Domain Keys Identified Mail (DKIM), and Sender policy for organisational email validation, which prevents spam by detecting email spoofing. Strong password policies and multi-factor authentication (MFA) must be enforced.

There should also be a strict external device usage policy in place and data-at-rest and data-in-transit encryption along with blocking attachment file types like .exe, .plf, or .url to avoid downloading malicious code.

The agency has also advised periodic security audits of critical networks/systems, especially database servers.