DREAMLAB TECHNOLOGIES

CYBER INSIGHTS

Research updates and insights from Dreamlab Technologies

In this issue:

Paragon spyware used to target individuals across European countries

The Italian government on 5 February 2025 reported that individuals in Italy, and several other European countries were targeted by spyware in a widespread hacking campaign uncovered by WhatsApp (Italian Government, 2025). WhatsApp, earlier in the week, revealed that the hacking campaign was carried out using spyware developed by Paragon Solutions, an Israeli firm, targeting around 90 users acrosscountries (Smalley, 2025), including Belgium, Greece, Latvia, Lithuania, Austria, Cyprus, Czech Republic, Denmark,Germany, the Netherlands, Portugal, Spain and Sweden (Italian Government, 2025).

Italy's National Cybersecurity Agency (ACN) investigated the hacking attempts, coordinating with WhatsApp and its law firm, Advant, to reveal the number of affected victims in Italy, which turned out to be seven.

The spyware, known as Graphite, developed by Paragon, is a military-grade commercial surveillance tool capable of automatically accessing encrypted messages and all information on a target's mobile, even without a user interaction (e.g., a click) (Kirchgaessner & Giuffrida, 2025). It is sold to government agencies, to allow them to track criminals. The Italian government denied any involvement in targeting victims (Italian Government, 2025), that reportedly include an investigative journalist, an advocate for migrants, and a Sweden-based Libyan activist critical of Italy. WhatsApp stated that a malicious PDF file was distributed among the targeted victims, to infect their phones, but the attack vector was shut down and the targets were informed. Paragon, however, declined to comment on WhatsApp's allegation that its spyware was used to target journalists and activists across Europe.

City in Texas suffers major cyberattack, Mayor urges state of emergency

The city of Mission, Texas, in the US suffered a major cyberattack on 28 February 2025 that compromised the city's entire network and data systems (The Attorney General, 2025), potentially risking exposure of sensitive personal and health information. On 4 March 2025, following the cyberattack, the city Mayor requested the Texas Governor to declare a state of emergency (City of Mission, 2025), to invoke extraordinary measures to address the situation, emphasising the severity of the attack.

The cyberattack, which caused the city's entire server and back up servers to be encrypted by ransomware, affected all city departments (The Attorney General, 2025), forcing systems offline, although emergency services continued to be in operation. Reports indicated that police officers lost access to key state databases, such as license plate and driver's license information, threatening the security of sensitive information, including civil, and criminal records. The emergency declaration was meant to allow temporary relief by suspending certain statutes, for more effective responses to mitigate the effects of the cyberattack. Third-party cybersecurity experts were reportedly engaged to handle the situation, alongside officials. With the growing number of cyberattacks on Texas cities, the Governor, earlier in February 2025 announced the creation of a 'Texas Cyber Command center' on a priority basis (Office of the Texas Governor, 2025).

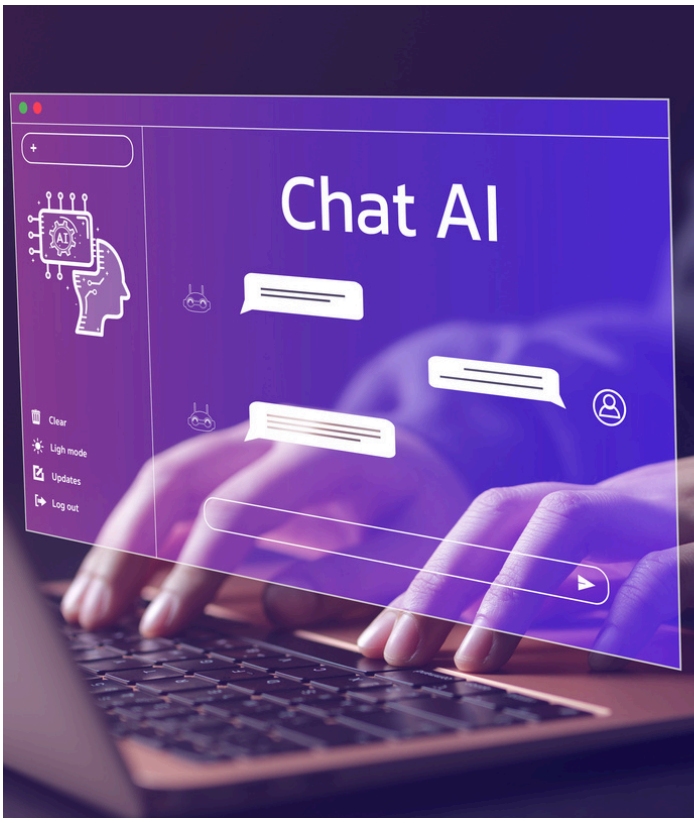
Singapore indicts three for fraud linked to suspected unauthorised transfer of Nvidia chips

Singapore, on 27 February 2025, charged three individuals, two Singaporeans and a Chinese national, with fraud linked to the suspected transfer of Nvidia's AI chips to the Chinese AI firm DeepSeek (Kok, 2025). The case is part of a broader investigation by Singapore into AI chip smuggling, involving several individuals and companies suspected of misrepresentation of the final destination of US-manufactured servers, to bypass trade restrictions. As per assessments, the servers likely contained Nvidia chips, supplied by US companies Dell Technologies and Super Micro Computer, which were then sent to Malaysia (Lok, 2025). The final destination of the servers, however, remains uncertain, and the Singapore government and US authorities are jointly working to determine it.

The charged individuals, if convicted could face up to 20 years in prison, fines, or both. The U.S. has been investigating whether DeepSeek has been using these US-made chips, which by are prohibited for export to China by regulations. Reports allege that DeepSeek may have acquired as many as 50,000 high-end Nvidia chips, though there has been no evidence to back the claim (Lok, 2025). DeepSeek denied these allegations, stating that the specific Nvidia chips it uses were legally purchased in 2023. Dell and Supermicro affirmed compliance with trade regulations, suggesting violation of regulations by a third party, while Nvidia declined to comment. Singapore has pledged to consistently enforce export control laws and prevent illicit activities.

Australia bans DeepSeek on national security grounds, China slams decision

The Australian government on 4 February 2025 banned DeepSeek, the Chinese AI chatbot, from federal government devices on grounds of national security (Australian Government, 2025). The ban requires blocking access and removal of DeepSeek products from government devices. The Chinese government has criticised the decision, accusing the Australian government of politicising trade and technology issues, while emphasising China's commitment to data security, and appealing for greater cooperation in technological development and innovation (Olbrycht-Palmer & Siyani, 2025).



DeepSeek, which gained attention for its efficiency and cost-effectiveness, reportedly fuelled a rapid increase in the adoption of artificial intelligence (AI) across China's high-tech manufacturing sector, including robots, and electric vehicles (EVs). However, it raised alarms due to its controversial and pro-Beijing responses on certain topics (Olbrycht-Palmer & Siyani, 2025). Moreover, it has been criticised for potentially collecting sensitive data, with reports suggesting that there are no safeguards in place for third-party data in its data collection clause (Olbrycht-Palmer & Siyani, 2025). The ban follows similar actions by Italy and Texas, with growing international concerns about the app's alleged privacy risks. The Australian government has urged citizens to be cautious about their online privacy and read privacy policies carefully.

Microsoft reports Silk Typhoon targeting IT supply chain, US charges malicious actors

Microsoft, on 5 March 2025, issued a warning against 'Silk Typhoon', the Chinese cyber-espionage group's new tactics, that now executes supply chain attacks, targeting remote management tools and cloud services (Microsoft, 2025). These attacks have been exploiting unpatched applications and stolen credentials to access downstream customer environments across sectors, often targeting Microsoft and other cloud services. The group has been observed exploiting multiple vulnerabilities, including a critical zero-day Ivanti Pulse Connect VPN vulnerability (CVE-2025-0282) in January 2025, and vulnerabilities in other third-party service providers, that caused the December 2024 U.S. Treasury Department breach (DOJ, 2025), leading to cyber-espionage activities.

The U.S. authorities on 5 March 2025, charged 12 Chinese nationals linked to hacking operations, including the Treasury Department breach and announced the seizure of internet domains linked to the Silk Typhoon group, also known as APT27 (DOJ, 2025). The criminal charges and domain seizures come after a series of alerts issued by the US government last year on Chinese cyberattacks on US networks including the huge telecoms breach, highlighting persistent targeting of U.S. interests by various hacking groups linked to China like Salt Typhoon, Volt Typhoon, and Silk Typhoon (Lyons, 2025). Microsoft has advised organisations to update their security tools with the latest patches to prevent cyberattacks, as Silk Typhoon continues to evolve its strategies.

Debopama Bhattacharya
Dreamlab Audit Team
Dreamlab Research Team

References

Australian Government (2025): Senate Legal and Constitutional Affairs Committee opening statement. Australian Government, accessed 10th March 2025, https://www.homeaffairs.gov.au/news-media/speeches/2025/25-february-senate-estimates

City Of Mission (2025): City of Mission disaster declaration. Office of the Mayor, City Of Mission, accessed 11th March 2025, http://missiontexas.us/wp-content/uploads/2025/03/DISASTER-DECLARATION-3.2.25-002.pdf

Italian Government (2025): Note of Palazzo Chigi. Italian Government Presidency of the Council of Ministers, accessed 6th March 2025, https://www.governo.it/it/articolo/nota-di-palazzo-chigi/27601

Kirchgaessner, S. & Giuffrida, A. (2025): Italian founder of migrant rescue group 'targeted with spyware'. The Guardian, accessed 10th March 2025, https://www.theguardian.com/technology/2025/feb/05/activists-critical-of-italian-pm-may-have-had-their-phones-targeted-by-paragon-spyware-says-whatsapp?utm_source=substack&utm_medium=email

Kok, X. (2025): Singapore charges three with fraud that media link to Nvidia chips. Reuters, accessed 3rd March 2025, https://www.reuters.com/technology/singapore-charges-three-with-fraud-that-media-link-nvidia-chips-2025-02-28/

Lok, B. (2025): US servers in Singapore fraud case may contain Nvidia chips, minister says. Reuters, accessed 3rd March 2025, https://www.reuters.com/technology/servers-used-singapore-fraud-case-may-contain-nvidia-chips-minister-says-2025-03-03/

Lyons, J. (2025): Feds name and charge alleged Silk Typhoon spies behind years of China-on-US attacks. MSN, accessed 7th March 2025, https://www.msn.com/en-us/news/world/feds-name-and-charge-alleged-silk-typhoon-spies-behind-years-of-china-on-us-attacks/ar-AA1AkLcX

Microsoft (2025): Silk Typhoon targeting IT supply chain. Microsoft, accessed 4th March 2025, https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

Office of the Texas Governor (2025): Governor Abbott Announces Texas Cyber Command An Emergency Item. Office of the Texas Governor, Greg Abbott, accessed 11th March 2025, https://gov.texas.gov/news/post/governor-abbott-announces-texas-cyber-command-an-emergency-item

Olbrycht-Palmer, J. & Siyani, H. (2025): Big issue with DeepSeek exposed after China envoy warns Australia against ban.News.com.au, accessed 11th March 2025, https://www.news.com.au/technology/online/big-issue-with-deepseek-exposed-after-china-envoy-warns-australia-against-ban/news-story/1f0292430f5ae190239f39a614c432cb?utm_source=substack&utm_medium=email

Smalley, S. (2025): WhatsApp accuses Paragon of targeting about 90 users with spyware. The Record from Recorded Future News, accessed 10th March 2025, https://therecord.media/whatsapp-paragon-spyware-targeting-users

The Attorney General (2025): City of Mission Catastrophe Notice. Ken Paxton, Attorney General of Texas, accessed 11th March 2025, https://www.texasattorneygeneral.gov/open-government/governmental-bodies/catastrophe-notice/catastrophe-notices/city-mission-2025-03-01

US Department of Justice (DOJ) (2025): Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns. US Department of Justice, accessed 6th March 2025, https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global

ISECOM

Member of the World Wide Web Consortium for security standards.

W3C

Board member of the Institute for Security and Open Methodologies.

UNIÓN EUROPEA

Research partner for EU cyber security research projects.

OWASP

Member of the Open Web Application Security Project.

INTERNATIONAL TELECOMUNICATION UNION

Sector Member of the UN's specialised agency for information and communication technologies.

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST)

Liaison Member.

SWISS MADE SOFTWARE

Officially certified as a provider of Swiss Made Software solutions.

CYBER SECURITY MADE IN EUROPE

Recognition of the quality of our cybersecurity services and products.

PARTNER CYBER SAFE

Audit partner for the label certification process.

FACHHOCHSCHULE NORDWESTSHWEIZ

Research partner for digital initiatives in Switzerland.

ALSEC

Specialized partner for critical operational technology (OT) infrastructures.

SLINF

Specialized partner of government security solutions.

GENEVA CHAMBER OF COMMERCE

Partner in investigation projects focused on e-commerce security solutions.

BLACK HAT

Member of the Review Committee at Black Hat International Cybersecurity Conference.

SWISS CYBER SECURITY DAYS

Founding Partner of the Swiss Cyber Security Days.

About Dreamlab Technologies

Dreamlab Technologies is a Swiss IT security company with locations on four continents. The combination of the Swiss technical capabilities as well as their international expertise enables Dreamlab to develop, assess and control cybersecurity based on quantifiable and verifiable open-standard technologies. Dreamlab advises organisations and authorities and helps them integrate information security awareness into their management cycle. In addition to its software products CyObs, CySOC and many other solutions, Dreamlab also offers IT security audits and training at all its locations.

Further information: https://dreamlab.net/

DREAMLAB TECHNOLOGIES

Monbijoustrasse 36
CH-3011 Bern
Tel: +41 31 398 6666
Fax: +41 31 398 6669
contact@dreamlab.net