AI поддржани APT напади - Скриената изложеност и ненамерната поддршка на телекомуникацискиот сектор

Никола Николов
Советник на директорот за информатички технологии

25.декември.2025

Table 1: GTMI Groups, 2025

GTMI Group		# of Economies	Economies
A	Extensive GovTech Maturity	80 (41%)	Albania; Argentina; Armenia; Australia; Austria; Azerbaijan; Bahrain; Bangladesh; Belarus; Belgium; Bhutan; Brazil; Bulgaria; Cabo Verde; Canada; Chile; Colombia; Costa Rica; Croatia; Cyprus; Czech Republic; Denmark; Dominican Republic; Ecuador; Egypt; Estonia; Finland; Germany; Greece; Hungary; Iceland; India; Indonesia; Ireland; Italy; Japan; Jordan; Kazakhstan; Kenya; Korea, Rep.; Kosovo◊; Latvia; Lithuania; Luxembourg; Malaysia; Malta; Mauritius; Mexico; Moldova; Mongolia; Netherlands; New Zealand; North Macedonia; Oman; Panama; Peru; Portugal; Qatar; Russian Federation; Rwanda; Saudi Arabia; Serbia; Singapore; Slovenia; Spain; Sweden; Switzerland; Tanzania; Thailand; Türkiye; Uganda; Ukraine◊; United Arab Emirates; United Kingdom; Uruguay; Uzbekistan
			France*; Norway*; Taiwan, China*; United States of America*

APTs

Lazarus Group

Article Talk

From Wikipedia, the free encycl

The **Lazarus Group** (also k
a state-sponsored hacker gr
the government of North Ko
have attributed many cybera

Originally deemed as a clan
as an advanced persistent t
methods used when conduc
organizations include **Hidde**
Homeland Security to refer t
in general),[4][5] **ZINC** and **D**
Korean defector Kim Kuk-so
Liaison Office.[10]

The Lazarus Group has stro
Department of Justice has c
strategy to "undermine globa
of ... sanctions".[13] North Ko
can present an asymmetric
Korea.[14]

Salt Typhoon is an advanced persistent threat actor believed to be operated by China's Ministry of State Security (MSS) which has conducted high-profile cyber espionage campaigns, particularly against the United States. The group's operations place an emphasis on counterintelligence targets in the United States and data theft of key corporate intellectual property. The group has infiltrated over 200 targets in over 80 countries.[1] Former NSA analyst Terry Dunlap has described the group as a "component of China's 100-Year Strategy."[2]

Organization and attribution [edit]

Salt Typhoon is widely understood to be operated by China's Ministry of State Security (MSS), its foreign intelligence service and secret police.[3][4] The Chinese embassy in New Zealand denied all allegations, saying it was "unfounded and irresponsible smears and slanders".[5]

According to Trend Micro, the group is a "well-organized group with a clear division of labor" whereby attacks targeting different regions and industries are launched by distinct actors, suggesting the group consists of various teams, "further highlighting the complexity of the group's operations."[6][7] The cyberattacks were reported to have commenced since at least 2023.[8]

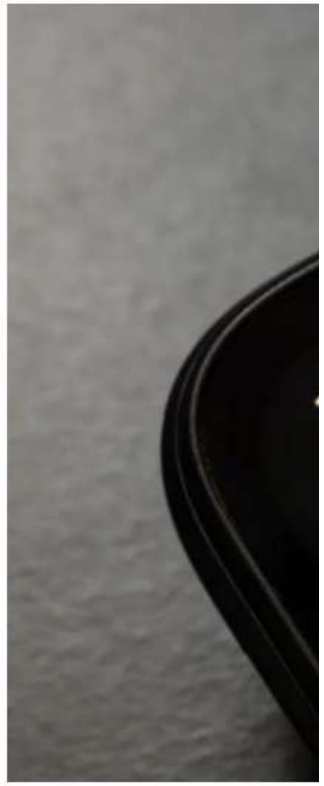
Salt Typhoon

Formation	c. 2020; 5 years ago
Type	Advanced persistent threat
Purpose	Cyber espionage, counterintelligence, data exfiltration
Location	China
Parent organization	Ministry of State Security
Affiliations	Sichuan Juxinhe Network Technology Co. Ltd. Beijing Huanyu Tianqiong Information Technology Co., Ltd. Sichuan Zhixin Ruijie Network Technology Co., Ltd.

AI firm claims Chinese spies used its tech to automate cyber attacks

14 November 2025

Joe Tidy
Cyber corresponde



The makers
sponsored by
attacks agair

Initial access [edit]

To gain initial access into their targets, the group has been observed exploiting known vulnerabilities in firewalls, routers, and VPN products:[30][31]

CVE	Description
CVE-2024-21887	Ivanti Connect Secure and Ivanti Policy Secure web-component command injection vulnerability
CVE-2024-3400	Palo Alto Networks PAN-OS GlobalProtect arbitrary file creation leading to OS command injection.
CVE-2023-20273	Cisco Internetworking Operating System (IOS) XE software web management user interface post-authentication command injection/privilege escalation
CVE-2023-20198	Cisco IOS XE web user interface authentication bypass
CVE-2018-0171	Cisco IOS and IOS XE smart install remote code execution
CVE-2021-26855	Microsoft Exchange Server Server-Side Request Forgery Vulnerability (ProxyLogon)
CVE-2022-	

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

AI firm claims Chinese spies used its tech to automate cyber attacks

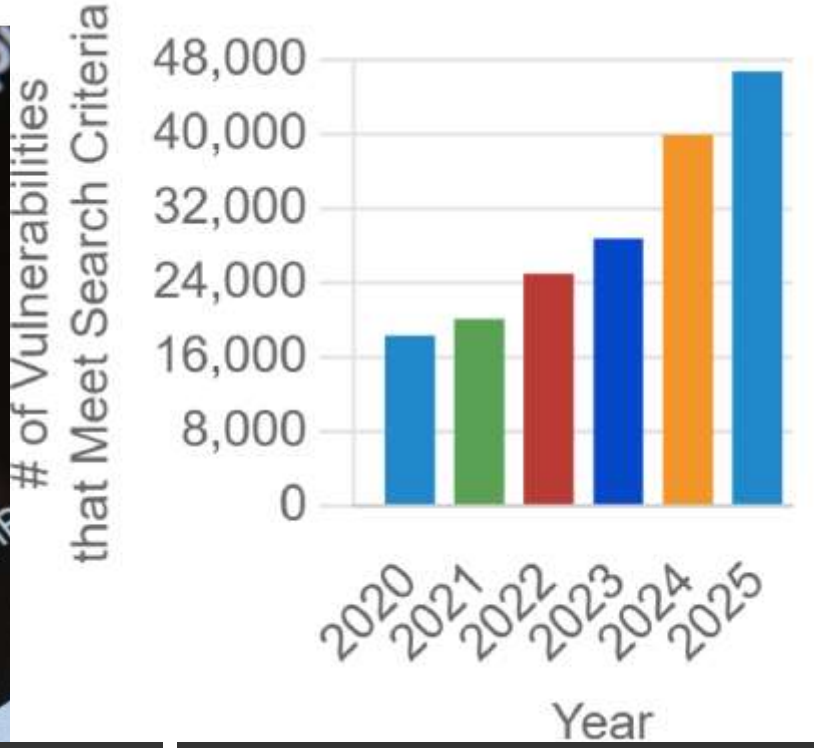
14 November 2025

Share Save

Joe Tidy
Cyber correspondent, BBC World Service

The makers of artificial intelligence
sponsored by the Chinese governme
attacks against around 30 global organisations

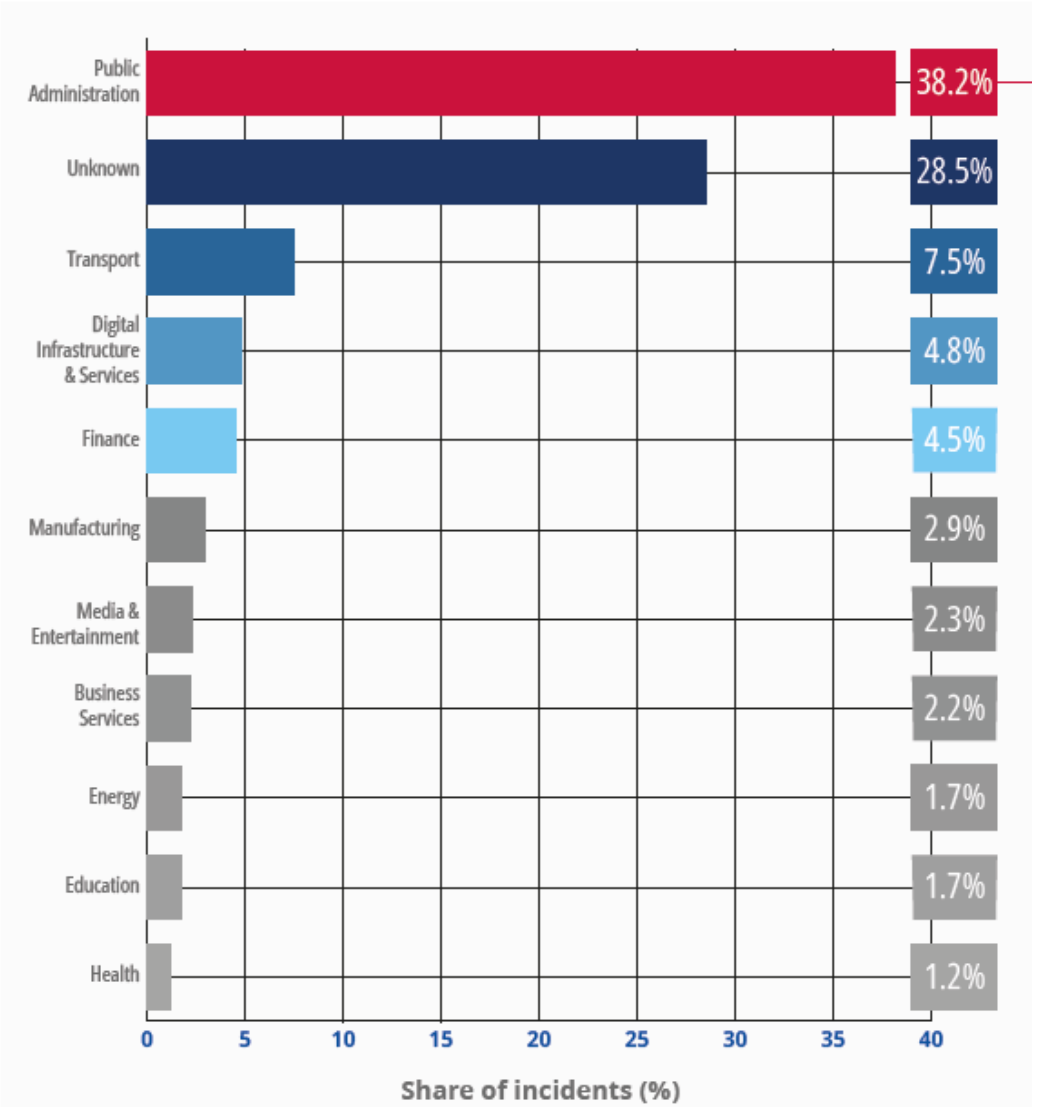
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



2024
Number of Vulnerabilities: 39972

2025
Number of Vulnerabilities: 46781

Sectorial overview



Share of recorded incidents by sector

Source: ENISA dataset

Salt Typhoon

infiltrated +200 targets

+80 countries

BBC

The Register

JLR: Payroll data stolen in cybercrime that shook UK economy

Automaker admits raid that crippled its factories in August led to the theft of sensitive info

Carly Page

Mon 15 Dec 2025 // 12:08 UTC

Jaguar Land Rover (JLR) has reportedly told staff the cyber raid that crippled its operations in August didn't just bring production to a screeching halt – it also walk off with the personal payroll data of thousands of employees.

The breach, which has been pegged as one of the most costly in UK history, include bank account details, tax codes, and other sensitive data related to staff salaries, benefits, and former employees.

In an email to both current employees and former employees, seen by *The Telegra* JLR wrote: "While investigating, we have unfortunately identified that there has bee unauthorised access to some personal data we process in the context of employm and some information needed to administer payroll, benefits and staff schemes to employees and dependents. This includes data of ex-JLR team members that has b stored."

Cyber correspondent, BBC World Service

dio Video Live

everely

Share Save

The Register

Beyond JLR's own balance sheet, the damage rippled outward: the Cyber Monitoring Centre has classed the incident as a systemic event that could cost the UK economy up to £2.1bn, while Office for National Statistics data shows motor vehicle manufacturing shaved 0.17 percentage points off GDP in September, helping tip the economy into contraction.

The attack was attributed to Scattered Lapsus Hunters, the same hacker group responsible for other major incidents, including attacks on Marks & Spencer and the Co-op. The hackers claimed they also stole customer data, but JLR has yet to confirm or deny this and did not respond to *The Register*'s repeated calls for comment on Monday.

The breach is yet another reminder of the growing vulnerability of major corporations to cyber threats, especially those outsourcing critical cybersecurity functions. ®

270 2.7K 27K 136K

Affected Population