1. Salt Typhoon: All about the Chinese hackers who targeted the 2024 US election

Introduction

A sophisticated breach of U.S. telecommunications systems has extended to the presidential campaigns, raising questions about the group behind the attack and the extent of its efforts at collecting intelligence.

It was unclear what data was taken in the attack. The far-reaching operation has been linked to the Chinese government and attributed to a group experts call Salt Typhoon. Investigators believe hackers took aim at a host of well-connected Americans, including the presidential candidates — reflecting the scope and potential severity of the hack.

What is Salt Typhoon?

Salt Typhoon is the name Microsoft cybersecurity experts have given to a Chinese group suspected of using sophisticated techniques to hack into major systems — most recently, US telecommunication companies. The moniker is based on Microsoft's practice of naming hacking groups after types of weather — "typhoon" for hackers based in China, "sandstorm" for efforts by Iran and "blizzard" for operations mounted by Russia. A second term, in this case "salt," is used to denote the type of hacking.

Experts say Salt Typhoon seems to be focused primarily on counterintelligence targets, unlike other hacking groups that may try to steal corporate data, money or other secrets.

What do US officials think Salt Typhoon has done?

National security officials have gathered evidence indicating the hackers were able to infiltrate major telecom companies, including but not limited to Verizon.

The New York Times reported Friday that among the phones targeted were devices used by former President Donald Trump and his running mate, Sen. JD Vance of Ohio. The effort is believed to be part of a wide-ranging intelligence-collection effort that also took aim at Democrats, including staff members of both Vice President Kamala Harris' campaign and Sen. Chuck Schumer of New York, the majority leader.

How serious is this hacking?
National security officials are still scrambling to understand the severity of the breach, but they are greatly concerned if, as it appears, hackers linked to Chinese intelligence were able to access U.S. cellphone and data networks. Such information can provide a wealth of useful intelligence to a foreign adversary like China.

To some degree, the breach represents a continuation of data collection on the types of targets that spies have been gathering for decades. In this instance, however, the sheer quantity and quality of the information Salt Typhoon may have gained access to could put the intrusion into its own category, and suggests that U.S. data networks are more vulnerable than officials realized.

What did the hackers get?
At this stage, that is still unclear. One major concern among government officials is whether the group was able to observe any court-ordered investigative work, such as Foreign Intelligence Surveillance Act collection — a highly secretive part of American efforts to root out spies and terrorists.

No one has suggested yet that the hackers were able to essentially operate inside individual targets' phones. The more immediate concern would be if they were able to see who was in contact with candidates and elected officials, and how often they spoke and for how long. That kind of information could help any intelligence agency understand who is close to senior decision-makers in the government.

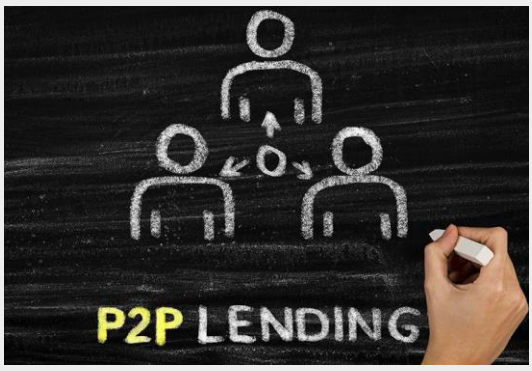
People familiar with the investigation say it is not yet known if the hackers were able to gain access to that kind of information; investigators are reasonably confident that the perpetrators were focused on specific phone numbers associated with presidential campaigns, senior government leaders, their staff members and others.

Like the weather, hacking is never really over, and the Salt Typhoon breach may not be over either. It is also possible that the United States may never learn precisely what the hackers got.

Relevance: GS Prelims & Mains Paper III; Science & Technology
Source: Indian Express

2. The rise and fall of P2P lending in India

Introduction



After the Reserve Bank of India's clampdown on peer-to-peer (P2P) exchanges in August this year, the industry's asset under management (AUM) plummeted by 35% — from an estimated ₹10,000 crore to ₹6,500 crore. No surprises there, since the RBI's restrictions targeted features that were most attractive to potential investors — tenure-linked assured minimum returns and liquidity options — apart from mandating T+1 settlement cycle. A P2P

platform's role is limited to facilitating transactions between lenders and borrowers without participating directly in the lending or borrowing process. While opinions differ on the industry's ability to comply with the new norms, businessline takes a look at the past, present and likely future of P2P lending in India.

Informal lending

Talk of regulating P2P lending first emerged in 2016, to curb informal money-lending. Citing the global pickup in P2P lending and newer entrants in India, the RBI floated a discussion paper on whether regulation was needed or not.

The arguments against included inadvertently lending credibility to P2P lending, with the stamp of regulation; stifling growth; and the absence of any immediate systemic risk from the nascent sector. After the feedback from stakeholders, the RBI in 2017 issued master directions on P2P lending in India, specifying the scope of activities for the lenders, eligibility criteria, and transparency and pricing disclosure requirement, among others.

What went wrong?

According to an RBI official, who requested anonymity, P2P exchanges began acting like a bank, drawing the ire of the regulator. They pocketed the spread between the borrowing rate and the interest that a lender charged on the platform. The RBI's restrictions soon followed. The regulator declared that P2P exchanges cannot utilise the funds of one lender to replace those of another, effectively killing the secondary market. It also stressed that P2P players must disclose their fees at the time of lending.

The RBI also disallowed the practice of matching and mapping participants within a closed user group, whether through an outsourcing agency or otherwise.

What lies ahead?

There are divergent views on the future of P2P lending in India. A large P2P exchange has stopped onboarding new customers since August 16, leading to 30-35 % loss in AUM, an official said. "RBI officials are visiting our offices to assess whether we are in compliance with the new norms. If some of the secondary market features are not revived, the industry may see a sharp fall in volumes. Large players like us are thinking of giving up the licence," a company official said.

But not all are pessimistic. Bhavin Patel, founder and CEO, LenDenClub, says in any regulated business some players will push boundaries till the industry reaches product-market fit.
"Auto-lending were discontinued, as it needed flow change, but it did not affect customers," he said.

Relevance: GS Prelims & Mains Paper III; Economics
Source: The Hindu

3. What is the Hibox 'investment' scam, in which Indians have lost Rs 1,000 crore?

Introduction

A large number of Indians are estimated to have lost a cumulative Rs 1,000 crore after being cheated in the so-called Hibox application scam, in which they were offered high interest on their "investments". The app was promoted by popular influencers on social media and YouTube, some of whom have been summoned by investigators.

The alleged scam is being investigated by the Intelligence Fusion and Strategic Operations (IFSO) unit, a specialised wing of the Delhi Police focused on cyber crime, which is also looking into the role of digital payments platforms PhonePe and Easebuzz, on which the alleged scamsters operated merchant accounts.

Hundreds of complaints received by police have been clubbed with FIRs registered in all the police districts of Delhi.

What is the alleged Hibox mobile app scam?
The modus operandi was simple and well worn. Would-be victims were invited to "invest" money through the app with the promise of extremely high returns. Early "investors" were rewarded with the promised amounts, which drew in more people, until one day the "returns" stopped coming and the individuals behind the app disappeared.

Police official explained how the alleged scam worked: "They (the alleged scamsters) lured victims with the help of social media influencers and YouTubers, convincing them to invest in their platform. The investors were promised guaranteed returns of 1 per cent to 5 per cent daily, amounting to 30 per cent to 90 per cent monthly.

"More than 30,000 people invested their hard-earned money in the Hibox app. However, the platform has since stopped releasing funds to the investors, and the companies have disappeared after closing their office in Noida," he said.

When did the alleged scam come to light?
On August 16, police received complaints from 29 persons at the IFSO unit, who said they were promised guaranteed daily returns of 1 per cent to 5 per cent.

"One thing that all the complainants said was they had decided to invest in Hibox after they found that the app was promoted by many social media influencers and YouTubers.

After conducting an initial inquiry into the complaints, police registered an FIR on August 20, and subsequently discovered that a similar FIR had been registered at the cyber police station of North Delhi, where nine persons complained of being cheated in similar manner.

What did the investigation find?
After details of payment gateways and bank accounts involved were collected, it was found that payment gateways Easebuzz and PhonePe were used to transfer moneys.

What is the current status of the investigation?
A look-out circular has been issued against the directors of Hibox, who are currently abroad. Tiwari said the role of Easebuzz and PhonePe are under investigation. Several YouTubers and social media influencers have been asked to join the investigation.

Relevance: GS Prelims & Mains Paper III; Economics
Source: Indian Express