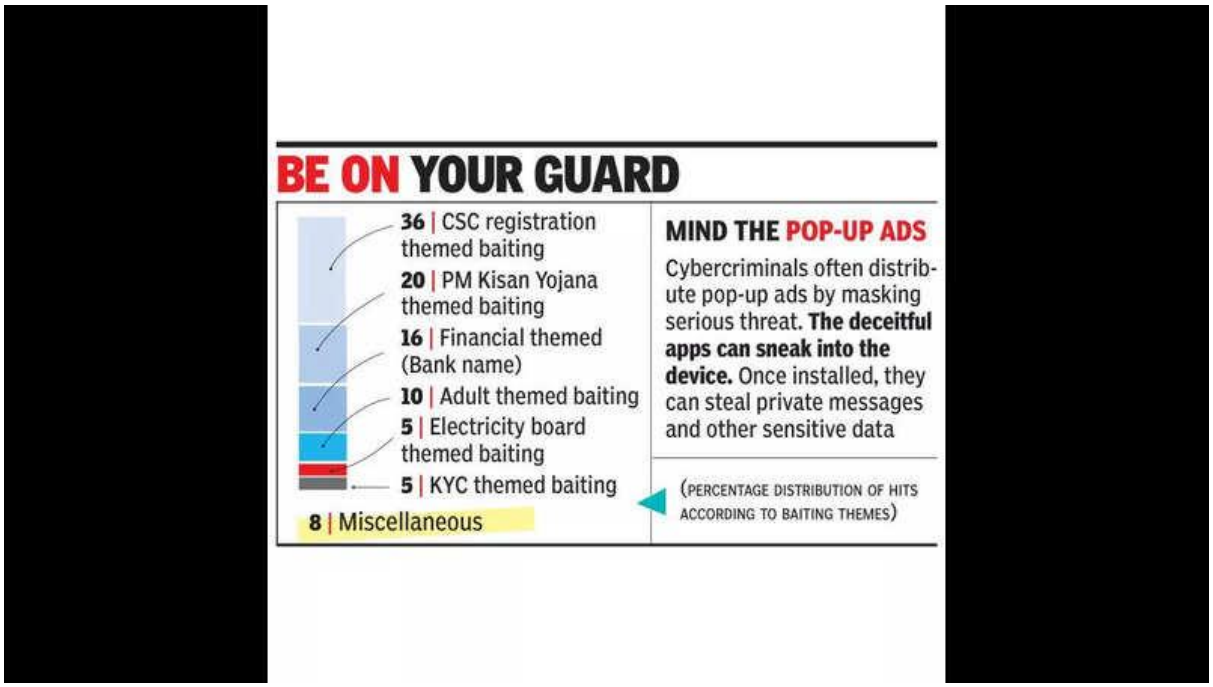
Govt agency' mask tops cybercrooks' con trick chart

Dec 17, 2024, 1:33 IST



Pune: Posing as central govt agencies to con people turned out to be the most favoured mode of operations for cybercriminals in 2024.

The govt entity type method of cyber con was found in 36% of cases out of the 37 crore malware detections across 84 lakh endpoints analysed by over 200 cybersecurity experts, showed data in a yearly cybersecurity threat report jointly released by Data Security Council of India (DSCI) and Seqrite.

Among other most used methods of duping the common man were the PM Kisan Yojana scheme at 20%, posing as bank representatives at 16%, and adult theme baiting at 10%.

"Govt push to digital India initiatives has been a great success, but the cybercriminals are using it to their advantage because of a lack of cyber awareness among the masses. If the source is a trusted one, then the victims are caught unawares. They only get to know about the con when they are cheated and lose financially," Lt Col Santosh Khadsare, CTO at DFIR SysTools, told TOI.

Digital fraudsters distribute malware files through WhatsApp by making fake representations of public sector banks, electricity boards, gas companies, and popular shopping malls. They lure the victims into installing harmful Android application package (APK) files by creating a false sense of urgency. The malware used by fraudsters is RewardSteal, named after the strategy of enticing users with promises of rewards to trick them into downloading infected files.

Additionally, cybercriminals also distribute pop-up ads promising secrets or useful insights by masking a serious threat. The deceitful apps can sneak into the device. Once installed, they can steal private messages and other sensitive data. If the stolen data includes sensitive financial information like bank verification codes or login credentials, the risk escalates, potentially leading to unauthorised access and identity theft.

"Our research also identifies cross-border threat groups like Anon Black Flag Indonesian and The Anonymous Bangladesh, with ransomware families like RansomHub and LockBit 3.0 leading the charge. Cyberattacks in tier 2 and tier 3 cities like Surat, Jaipur, and Ahmedabad have surged due to their growing significance as key economic and business centres," said Vishal Salvi, CEO, Quick Heal Technologies.

In the case of business entities, detection rates were highest in Telangana, followed by Tamil Nadu and Karnataka, as most attacks occurred in the industrial and technology belts. Telangana witnessed 56 detections per endpoint, followed by Tamil Nadu (45).

The detection rates were lowest in the two top Maharashtra cities — Mumbai (32) and Pune (30). The report highlighted that the lower instances of detection can mean that the reporting mechanism is not very extensive and many of the attacks and breaches are not reported on time.

"While ransomware continues to have a higher hit rate than other malware categories, its frequency has decreased compared to last year, indicating improved cyber resilience," cybersecurity expert Vinayak Godse said.