Cybercriminals target SMEs as large companies beef up security

Himanshi Lohchab, ETtechLast Updated: Sep 06, 2024, 06:00:00 AM IST

Synopsis

Attacks on small and medium enterprises (SMEs) (with 100-5,000 employees) have significantly risen in India and accounted for nearly half of all such incidents in 2023. Among large organisations, only 10% of those attacked paid ransom, whereas with SMEs, 44% ended up paying amounts ranging between $25,000 and $100,000, according to data from cybersecurity firms.

Cybercriminals are turning their focus to small and medium enterprises (SMEs) as large organisations bolster their cybersecurity infrastructure, maintain data redundancy, invest in cyber insurance, and refuse to pay ransom.

Hacker groups like Lockbit, BlackCat and Akira are increasingly targeting SMEs in healthcare, retail and manufacturing, who sometimes remain unable to regain their IT systems even after paying ransom.

Attacks on SMEs (with 100-5,000 employees) have significantly risen in India and accounted for nearly half of all such incidents in 2023. Among large organisations, only 10% of those attacked paid ransom, whereas with SMEs, 44% ended up paying amounts ranging between $25,000 and $100,000, according to data from cybersecurity firms.

“The impact of such attacks on SMEs can be devastating,” said Sanjay Katkar, joint managing director at cybersecurity software firm Quick Heal Technologies. “A cyberattack incurs heavy costs in terms of both finances and reputation, which is too much for most SMEs to recover from.” Cybercriminals'

exploitation of SMEs is a global trend, according to a study by digital security firm ESET. In 2023, cybercriminals deployed a record 500,000 unique malware daily on average. Incidents of cyber breach were the highest in India at 88%.

As per the annual surveys by security firm Sophos, nearly 64% SME organisations were attacked in 2023, lower than 73% in 2022. However, of those which were targeted, 65% ended up paying ransom in 2023 as against 44% the previous year. The amount paid as ransom has also increased substantially.

The mean ransom payment which stood at $194,400 in 2022 rose to $2,674,239 in 2023, while the median payment increased from $36,000 to $2,000,000, data showed.

“We are indeed witnessing a worrying trend where small and medium organisations are increasingly becoming prime targets for hackers,” said Sunil Sharma, vice president – sales at software security firm Sophos India and Saarc, adding that there have been instances where SMEs paid ransoms far beyond their capacity.

The rise of cybercrime as a service, where sophisticated tools like Cobalt Strike are sold to attackers through underground marketplaces, has democratised cyberattacks, making it easier for even less-experienced hackers to target SMEs, according to experts. “In the APAC region, SMBs face distinct cyberattack patterns, with system intrusion, social engineering, and basic web application attacks making up 92% of incidents,” said Anshuman Sharma, director at the Verizon Business Group.

“With SMBs accounting for over 56% of all cyberattacks, there is a critical need for improved cybersecurity measures to protect against these prevalent threats.” Supply chain attacks are increasingly targeting SMEs that serve as suppliers to larger enterprises, said Quick Heal’s Katkar. “These attackers exploit the weaker security postures of SMEs to gain access to the larger organisations they supply. This method has proven quite successful, as compromising one SME can provide a gateway into multiple large enterprises,” he said.

The shift to remote work has also expanded the attack surface for many SMEs, he added. Experts said in the absence of large security budgets, SMEs should focus on basic measures like multi-factor authentication, regular patching, employee training and enforcing strong password policies.