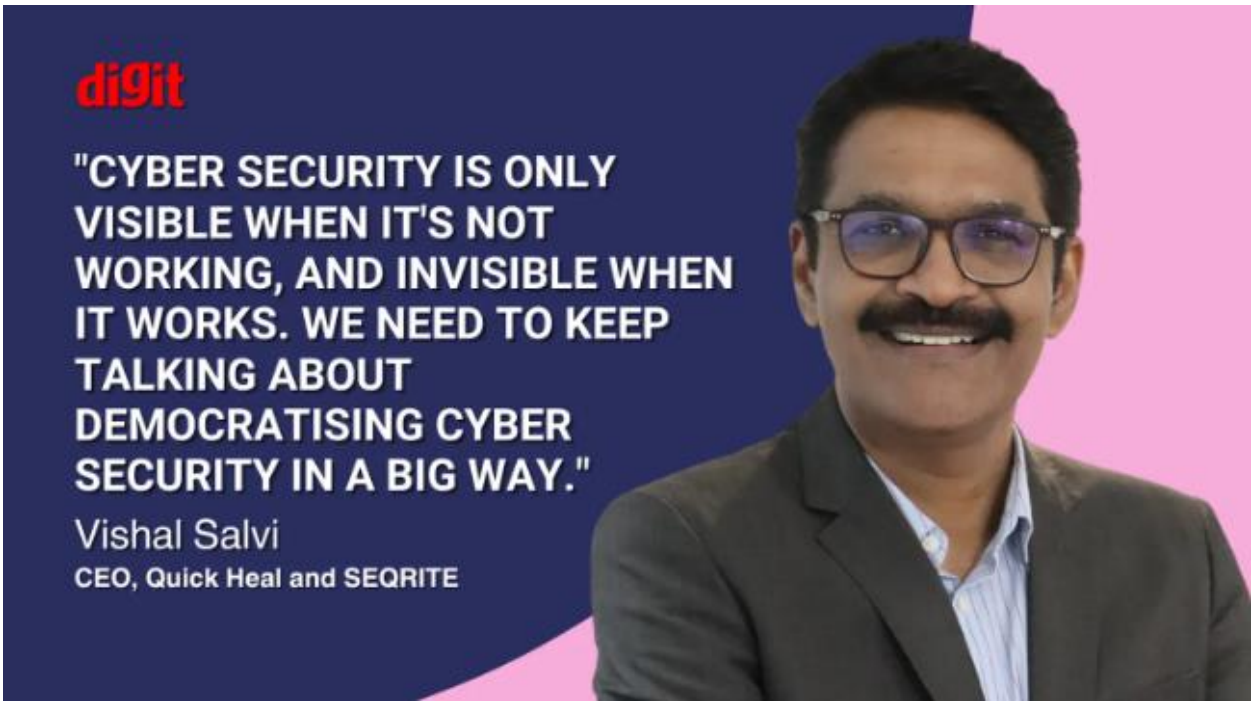
Quick Heal's Vishal Salvi on fighting malware to keep India cyber safe



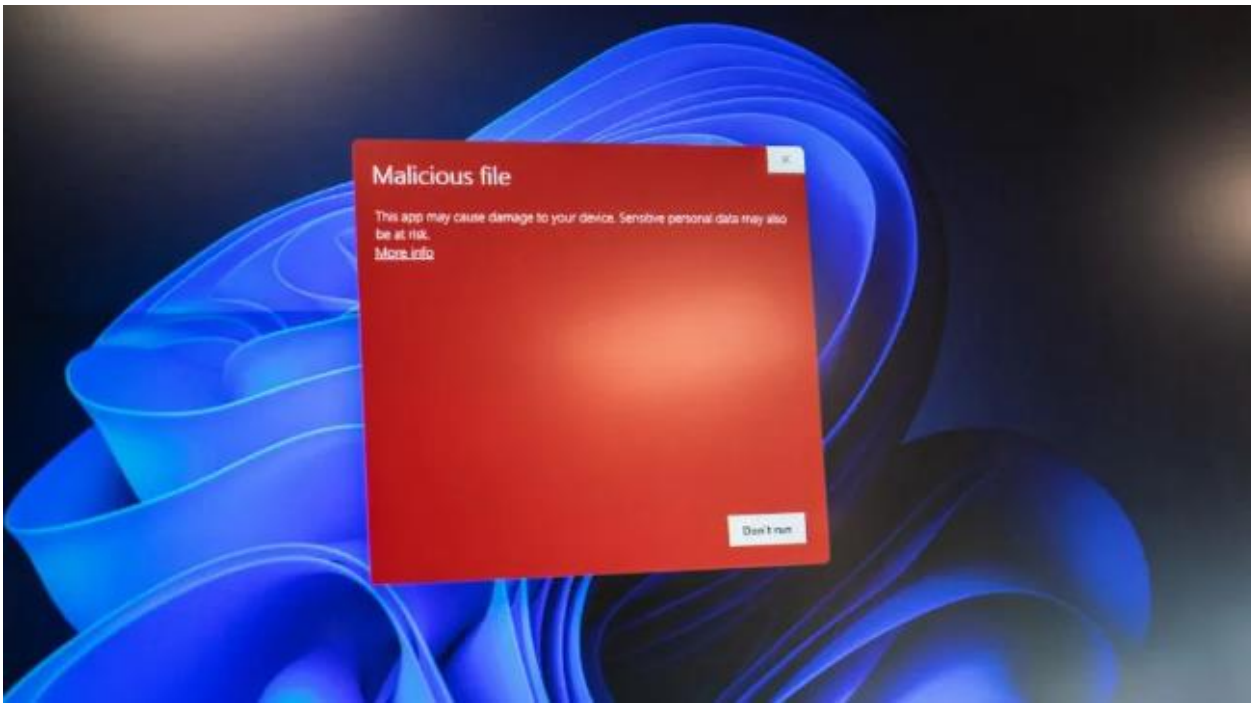
“It was obviously a very challenging software to be decoded, and we can discuss the technicalities of Expiro and what it really was, but I think it’s a testimony to the kind of capability and talent we have within the country. We are on par with any other cybersecurity vendor in the world, and it underlines the fact that we have the necessary capabilities in managing this cybersecurity event,” said Vishal Salvi, CEO, Quick Heal and SEQRITE.

He spoke to me in the backdrop of Quick Heal's recent breakthrough against the Expiro virus threats that made quite a few headlines, making them the only cybersecurity company to offer a comprehensive end-to-end solution against Expiro-related infections.

Experts at Quick Heal's Security Labs have not only analysed the latest version to understand how Expiro spreads, but also developed a complete solution to mitigate its impact. But what activities led to users and their systems getting infected in the first place? Did India’s love affair with pirated software play a significant part in Expiro virus’ propagation, I asked Mr Salvi.

“We have seen multiple traces of infections in all the deployments that we have done in India. We were at the forefront of looking at what this malware was doing, and malware does propagate through various methods – through the use of cracked software, drive-by downloads from infected websites, or even propagation through network shares, right?” said Salvi, suggesting the Expiro virus used all or any of these

techniques for propagation. And even though India's cyber sensibilities as a country are constantly growing in terms of use of legitimate software and understanding of secure controls and safeguards, "But there's always vulnerable infrastructure, vulnerable users, and that's really what we have seen in this case as well," he emphasised.



Fighting and weeding out Expiro's hidden mechanisms wasn't easy, Salvi told me. "When you look at an infector, it has two types broadly, one is called appender and the other prepender. Expiro was actually an appender virus, which are very rare compared to prepender," he explained, saying how appender infectors basically move around the header of any infected file. As a result, it becomes difficult to proceed in dealing with vulnerabilities effectively, he suggested. And that wasn't the least of Quick Heal's worries.

"The second complexity in case of Expiro was that it had multiple ports and functions which were called to create a significant amount of complexity," deliberately created for the good guys to get lost in the maze right while they were trying to reverse engineer a solution, according to Salvi. "Our team of analysts and researchers worked on this problem, they took it as a challenge to really understand how all of this was unfolding. And eventually, found a way to go back and restore the file to its original form. And that's really how we identified the detection, and within a matter of a few weeks we could then come up with a remediation technique," he stressed.

This isn't the case only with the Expiro virus, Salvi told me, but about any malware code that comes to Quick Heal's Security Labs. "We put all our effort to make sure that we are able to reverse engineer and address the problem. We are glad that we are the first to sort of solve this [Expiro virus] problem and perhaps the only company so far. It can only happen when you have things working together, with the right investments and the focus we have had in this topic, it augurs well for the future of our team. Itt gives us a lot of confidence in solving a complex threat like this which we believe is going to be the norm in the future," said Salvi.

Hearing from the head of a cybersecurity company that future threats are going to be more complex isn't easy. How is the industry, both public and private enterprise, including the Indian government, assessing the threat landscape, we asked Mr Salvi – who provided a reassuring response.

"We are obviously, you know, talking to all our stakeholders to see how some of the work that we're doing can be leveraged to keep them safe. And we've always been at the forefront of collaborating with any government bodies or corporate bodies, for helping them in understanding cyber threats in much more detail and depth. We engage in capacity building measures with the Data Security Council of India (DSCI) with their Cyber Surakshaa program and help in terms of training and nurturing talent and making them understand cybersecurity fundamentals, techniques and solutions," Salvi said, emphasising Quick Heal's commitment to playing an important role in terms of capacity building as far as the nation is concerned, and also building an indigenous make in India story in the cybersecurity domain.

Salvi has been quite vocal about democratising cyber security at every opportunity he gets to talk about it, especially related to making cyber security everyone's responsibility in some way shape or form. "What generally happens is there's a cybersecurity team, and the rest offload their responsibility on them. All the work that I expect to be done in order to keep me safe is designated to cyber security teams, but unless you are participating in the process of being cyber safe and understand your role, take ownership and accountability of your role, it becomes very difficult to really implement cybersecurity in a holistic way," he said, which is why democratising cybersecurity, making sure every stakeholder understands their role is very critical.

“Cybersecurity is only visible when it's not working, and it's invisible when it's working. Not getting hacked doesn’t mean you may not be vulnerable to that possibility, so it’s very important that every stakeholder understands responsible cyber security practices, especially given the fact that there's so much digital adoption in the country. We need to keep talking about it and spread the message about democratising and making people accountable for cyber in a big way,” Salvi emphasised.

But it isn’t all doom and gloom, especially as far as India is concerned, according to Salvi. “I'm extremely encouraged by the amount of enthusiasm and passion that young entrepreneurs in India are displaying by venturing into building cybersecurity solutions,” he said enthusiastically, recalling how a FinSec conclave he attended in Mumbai recently had lots of young Indian talent, creating various solutions and services on cybersecurity which was nothing short of amazing and extremely fascinating to him.

“It has never been like this, and it feels like we’re creating a Silicon Valley here in India for cybersecurity entrepreneurs. I think the time is right, you know, because we've done that in the IT services space before. As Quick Heal, we’re playing our part in giving direction to young entrepreneurs who want to pursue their ambition towards building security solutions not just for India but the world,” Salvi concluded.