Source : www.thehindu.com Date : 2021-08-06

# KASEYA RANSOMWARE ATTACK SETS OFF RACE TO HACK SERVICE PROVIDERS - RESEARCHERS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Image used for representation purpose. | Photo Credit: Reuters

A ransomware attack in July that paralysed as many as 1,500 organisations by compromising tech-management software from a company called Kaseya has set off a race among criminals looking for similar vulnerabilities, cyber security experts said.

*(Subscribe to our Today's Cache newsletter for a quick snapshot of top 5 tech stories. Click here to subscribe for free.)*

An affiliate of a top Russian-speaking ransomware gang known as REvil used two gaping flaws in software from Florida-based Kaseya to break into about 50 managed services providers (MSPs) that used its products, investigators said.

Now that criminals see how powerful MSP attacks can be, "they are already busy, they have already moved on and we don’t know where," said Victor Gevers, head of the non-profit Dutch Institute for Vulnerability Disclosure, which warned Kaseya of the weaknesses before the attack.

"This is going to happen again and again."

Gevers said his researchers had discovered similar vulnerabilities in more MSPs. He declined to name the firms because they have not yet fixed all the problems.

Also Read | Hackers exploit Kaseya ransomware attack to launch spam campaign

Managed service providers include companies such as IBM and Accenture offering cloud versions of popular software and specialist firms devoted to specific industries. They typically serve small and medium-sized firms that lack in-house technology capabilities and often boost security.

But MSPs also make an efficient vehicle for ransomware because they have wide access inside many of their customers' networks. Kaseya's software serves many MSPs, so the attacks multiplied before Kaseya could warn everyone, rapidly encrypting data and demanding ransoms of as much as $5 million per victim.

The business of MSPs has boomed during the coronavirus pandemic alongside the rapid increase in remote work.

"That's where you find the trusted access to customers' systems," said Chris Krebs, the first leader of the U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA), which has made ransomware a top priority. "It's a much more economical approach to launch a breakout attack. And it's hard for the customer to defend."

Bugcrowd Inc, one of several platforms where researchers can report vulnerabilities, has also seen security flaws as bad as Kaseya's, said Bugcrowd Chief Executive Ashish Gupta, perhaps because MSPs have been growing so fast.

"Time to market is such a high requirement, and sometimes speed becomes the enemy of security," Gupta said.

Also Read | US and allies accuse China of global hacking spree

Service providers have been targeted before - most dramatically by suspected Chinese government hackers who went after big tech companies in a series of breaches known as Cloud Hopper.

REvil hit more than 20 Texas municipalities through a shared provider two years ago, but only demanded $2.5 million in total ransom, said Andy Bennett, then a state official managing the response.

With REvil extortionists asking for a record $70 million to reverse all the Kaseya damage, he said, "their aspirations are clearly bigger now, and their approach is more measured." It's unclear how much ransom was ultimately paid or how many businesses were affected.

An increase in ransomware attacks led U.S. President Joe Biden to warn Russian President Vladimir Putin that the United States would act on its own against the worst hacking gangs operating on Russian soil unless the authorities reined them in.

On July 22, Kaseya said a security firm had developed a universal decryption key without paying the criminals, prompting speculation that Putin had helped or that U.S. agencies had hacked REvil.

Also Read | U.S. launches online hub to help ransomware victims

CISA is trying to get the word out both to MSPs and their customers of the risks and what to do about them, said Eric Goldstein, executive assistant director for cybersecurity.

Less than two weeks after the July 2 Kaseya attack, CISA issued guidelines for best practices on both sides of the equation. CISA also offers free risk assessments, penetration testing and analyses of network architecture.

"Organisations need to look into the security of their MSPs," Goldstein said. "The broader consideration here is the importance for organisations big and small to understand the trust relationships that they have with those entities that have connections into their environment."

**END**