

The count of managed service providers getting hit with ransomware mounts



Enlarge / When MSPs get owned by ransomware, their customers can lose more than just access to an application.

Getty Images

reader comments

32 with 25 posters participating

Share this story

When more than 20 local governments in Texas were hit this summer by ransomware in one day. The attack was apparently tracked back to one thing the organizations had in common: a managed service provider. With limited IT resources of their own, local governments have increasingly turned to MSPs to

operate significant portions of their networks and applications, as have other organizations and businesses—often placing critical parts of their business operations in the MSPs' hands. And that has made MSPs a very attractive target to ransomware operators.

Threat researchers at the global cloud security provider Armor have been tracking publicly-reported incidents in which MSP and cloud service providers have been hit with ransomware. Thus far, they have documented 13 such incidents this year—with 6 of them reported in the past few months.

The most recent publicly exposed victim is Billtrust, which as security journalist Brian Krebs reported, was hit by what BleepingComputer reported was BitPaymer ransomware (a report that has not been confirmed). BillTrust is an online invoicing and billing provider based in New Jersey that also provides credit decision services. Billtrust executives sent an email to customers on October 22, informing them of the attack, stating:

Our standard security and back-up procedures have been and remain instrumental in our ability to execute the ongoing restoration of services... Out of an abundance of caution, we cannot disclose the precise ransomware strains but will do so as soon as prudently possible.

Other victims include:

- SchoolinSites, a cloud-based service provider for school districts that offered websites and parental access to student information, was taken down in an attack in September as reported by WKRG in Mobile, Alabama. The company's email was affected as well as other communications; SchoolinSites had to use Facebook to provide updates during the outage, which began on September 23.
- TrialWorks, a Florida-based case management software

provider, was hit by a ransomware attack the week of October 14. The company, which serves about 2,500 law firms, acknowledged the ransomware attack and said that, while it did not impact their software, about 5% of the company's customers could not access their accounts.

- California-based MetroList, a real estate multiple listing and application services firm with about 20,000 real estate broker customers, was hit by ransomware in June, taking the company's services offline for two days. MetroList reportedly paid the ransom, which included a \$10,000 insurance deductible.
- Also on October 14, Magnolia Pediatrics of Prairieville, Louisiana, was reportedly hit by ransomware via the practice's managed IT services provider. Magnolia reported the ransomware to law enforcement.
- In July, CorVel, a managed service provider for insurance companies handling workers compensation, auto, health, and disability claims, got hit by Ryuk ransomware. As the company responded, systems used to process claims, email and phone systems, and healthcare provider databases were taken offline.

Organizations using full-service IT-managed service providers, such as Magnolia Pediatrics, are particularly at risk because the security of all of their systems is dependent on that of the MSP. As was the case in Texas, this meant that all their data was put at risk. In Magnolia's case, all patient data was encrypted, but it could just as easily have been stolen by attackers—and since that data includes personal identifying data for children, it could have significant long-term consequences. A clinic spokesperson said that “out of an abundance of caution,” Magnolia advised patients' families to monitor credit card statements and credit bureau reports.

These issues are why having a conversation (and a contract) with a service provider that includes security is so important.

<https://arstechnica.com/?p=1594073>