Written by Frederick Douglas
28 February 2020

Remote monitoring and management (RMM) platforms face a growing malware threat, Asigra warns, since an "incessant" stream of malware variants is putting both MSP and end-customer applications and data at "significant" risk.

RMM software helps MSPs remotely and proactively monitor client endpoints, networks and computers. Formerly known as remote IT management, RMM requires an agent installed on client servers, hypervisors, workstations, networking devices, laptops and other mobile endpoints. In case of problems, the RMM issues tickets or alerts the MSP classified according to severity, problem type and criticality.

Such solutions are very popular among MSPs globally, and for good reason. However the use of an RMM platform with tightly integrated backup solutions creates a single access point to dozens, hundreds or even thousands of organisations. According to Asigra, since RMM platforms push out agents, ransomware can potentially push out malicious code to each MSP client while neutering the backups.

Criminal hackers can compromise RMM admin privileges using tried and tested methodologies sucha s phishing, website hijacking or malicious advertising. For instance, they can send an urgent email or text appearing to be from a direct manager or company executive. The email or text would contain a link to download ransomware or malware, or an infected attachment. The email can also emulate an alert message from the RMM program. Either way, once the RMM platform is compromised, so is the integrated backup, and the entire MSP client base is under threat.

How can one mitigate such a threat? Asigra, of course, has some suggestions in the shape of a three-step process. First, all employees should be trained to be aware of phishing attacks. Second, all data protection infrastructure/solutions should be separate from the RMM platform. Integrated solutions should also be avoided. Finally the backup solution in use should be able to prevent ransomware and malware from deleting backups, as well as prevent such infections in the first place by scanning both backup and recovery streams.

“In many technology segments the centralisation of computing processes provides great value. However, tight integration of RMM and data protection is an area where extreme caution is warranted when it comes to backup/recovery design," the company adds. "The density of high value data in many RMM environments is too alluring for criminal hackers to avoid, making it incumbent upon the MSP to architect a bulletproof data recovery model. For the strongest protection, services professionals are advised to disentangle RMM and backup to ensure system recoverability.”

Go Asigra Warns that RMM Platforms with Integrated Backup Will be Ongoing Attack Vector for Ransomware in 2020