ActZero

Remote Monitoring and Management (RMM)

Reducing the Attack Surface

Remote monitoring and management tools are increasingly used by enterprises and/or their managed service provider to remotely manage endpoints including laptops and servers. For many they are an essential tool for connecting remotely, monitoring performance, performing software updates, resets, or recovery, identifying newly joined devices, and running diagnostic tests.

The ideal attack surface

As with most tools, as they become increasingly popular with businesses, they also gain the attention of those adversaries looking to disrupt the business. So, What makes RMM so appealing is their reach within the organization? Firstly, RMMs are connected to most every device and person in the organization. They're ubiquitous, and are able to install programs on large numbers of machines by design. From a security standpoint, they are rarely limited in their privileges on devices, are sometimes from antivirus scans, usually have protections turned off during updates, and are generally overlooked by security administrators. This is an ideal playing field for those looking to deploy ransomware, living off the land attacks, or more.

Through 2020 and 2021, we've seen a number of remote monitoring and management tools fall victim to cyber attacks. Kaseya and SolarWinds were two of the most notable solutions breached - not only affecting them, but their clients and supply chain as well. So how do these attacks occur, and what can you do about them?

How attacks on RMMs work

While there is no specific checklist or outcomes classifying an attack on an RMM, complicated more given there are so many variants of deployment and operation models, RMM hijacking often allows adversaries the ability to:

- Change code to cause the RMM to connect to their own malicious server rather than the target organization's legitimate one
- Take control of the remote management tool to gain access to targeted machines (often that of an executive)
- Install their own software on controlled machines, usually without detection
- Spread their control from one machine to others
- Pull files off of the RMM or machines for which it gains access
- Install malware, like ransomware, to drop their payloads into your environment, or that of your supply chain and partners'.

> "Any time you're using a system to manage many different devices, giving administrative control, it becomes imperative that that system is configured and managed securely."
>
> - Aaron Kiemele, CISO, JAMF

The biggest challenge of detecting threats on RMM

There are many reasons why automated detection tools like endpoint detection and response (EDR), network detection and response (NDR), or even SIEM find it difficult to find threats. The main reason: the expected behavior of an RMM is to be in regular contact with many devices on the network — changing configurations, installing or even deleting programs — making it very difficult to distinguish between approved and malicious activity.

Mitigating the risk

There is no absolute solution for protecting RMM tools from attack. To claim so would be irresponsible. However, there are some steps you can take to mitigate your risks.

Assess your tools and your vendors
Find out what tools and services your vendors are using in your network, and their own. This is critical as threats can easily jump between business partners, vendors and suppliers. Kaseya was a perfect example of this. We spoke about threats that jump from endpoints to cloud and beyond in our last Threat Insight piece.

Consider moving to the cloud
Shifting to the cloud-based RMMS tools can help prevent network-wide attacks. While a cloud-based RMM tool in and of itself is not a cybersecurity measure, it can help MSPs keep closer control over data and user access to their systems. If a cybersecurity incident occurs, businesses can know that their data is still intact in the cloud, log out all accounts, change user passwords, or take other actions making it difficult for hackers to attack multiple systems at one time.

Avoid single-purpose cybersecurity tools
Adopt cybersecurity tools that integrate directly with your RMM products, or have visibility to them so that IT experts can directly run security scans from the RMM portal. And make sure all RMM software and tools are updated with the latest security patches.

Apply regular access hygiene
Regular security hygiene practices for RMM is critical. Limit admin accounts, prioritize authentication security, and apply strict password policies to mitigate account takeover risks.

Employ a Managed Detection and Response solution
MDR providers, like ActZero, provide a valuable option for protecting your environments operating with an RMM. At ActZero, we use machine learning to enable anomaly detection techniques, which helps determine if activity chains and installation methodologies are unusual in any given RMM environment. his information is in turn used to guide our threat hunters in their search and validation of threats - finding and remediating them much quicker than human detection alone. We then use those learnings to continuously improve our capabilities — helping detect, stop, and communicate threats quicker each time.

To learn more about RMM attacks, and ActZero protects against them, stay tuned for our upcoming blog, or contact us now.

Email: info@actzero.ai
Phone: +1.855.917.4981