TRINITY CYBER

Legitimate Tools with Malicious Uses

Remote Monitoring and Management (RMM) tools have been around for many years. You've probably used them to get help from the IT department or to fix a family member's computer. Unfortunately, cyber actors also use RMMs to gain instant access to computer systems – and these attacks are growing as **a widespread vector for cyberattacks.**

Trinity Cyber has seen and stopped an increase in malicious campaigns that use RMMs. **Modern attacks usually start with a phishing lure;** a link that directs the user to a malicious website to download RMM software. The key to the attack is the RMM coming from a malicious place on the internet. RMMs offer natural camouflage as a legitimate tool, often overlooked by traditional detection mechanisms.

The Tools

Months of research led the Trinity Cyber team to the following list of most abused RMMs, which we stop with Full Content Inspection™ (FCI):

- ConnectWise ScreenConnect
- N-Able
- FleetDeck
- LogMeIn
- PDQ Connect
- Atera
- Datto (CentraStage)
- SyncroMSP
- ITarian
- SimpleHelp
- NetSupport Manager

The Lures

Phishing attacks that deliver RMMs have some consistent themes which are purpose-built to trick users.
Here's the most common:

- Social Security notifications
- IRS and tax updates
- CAPTCHA verification (ClickFix)
- eCards
- Email invitations
- Fake browser updates or "missing font" messages
- Meeting invitations including Zoom and Teams
- Invoices
- Shipping notifications

Light at the End of the Tunnel

Users don't often realize they're being targeted by cyber criminals with RMMs. These attacks get stealthier by the day, and are often assisted by modern AI systems. Trinity Cyber's Active Network Defense platform, powered by Full Content Inspection (FCI) is your best solution to RMM attacks. **FCI prevents these attacks before they reach users**, with a growing list of RMM coverage. This means legitimate RMMs go through, and malicious RMMs fail to attack your users.

Ready to learn more? Contact us today to schedule a live demo: sales@trinitycyber.com