TRINITY CYBER

Blending In: How Remote Monitoring and Management Tools Attack Your Network

Author: Mitch Edwards

Executive Summary

Threat actors are scaling up their use of legitimate Information Technology (IT) administration tools, such as Remote Monitoring and Management (RMM) software, to gain and leverage unauthorized access to victim endpoints and networks. These tools make the perfect backdrop for blending into corporate environments. They deploy RMMs as part of initial access – gaining control over multiple systems to carry out attacks that aim to:

- Establish persistent and long-term access
- Remotely spy on victims
- Steal proprietary information
- Deploy further malware (Ransomware, Infostealers, etc.)

Legacy detection methods lack context and are ill-equipped to handle malicious RMM threats. Public attention focuses on complex, multi-stage malware that hits the news and makes waves, while the malicious use of RMMs and other IT software flies under the radar. Over the past year, Trinity Cyber has observed and prevented a large increase in RMM attacks, using Full Content Inspection™ (FCI) to thwart malicious campaigns. These attacks typically start with phishing or Search Engine Optimization (SEO) poisoning attacks designed to funnel victims into download websites.

Each RMM campaign has a story; this analysis exposes some of their tactics.

Background

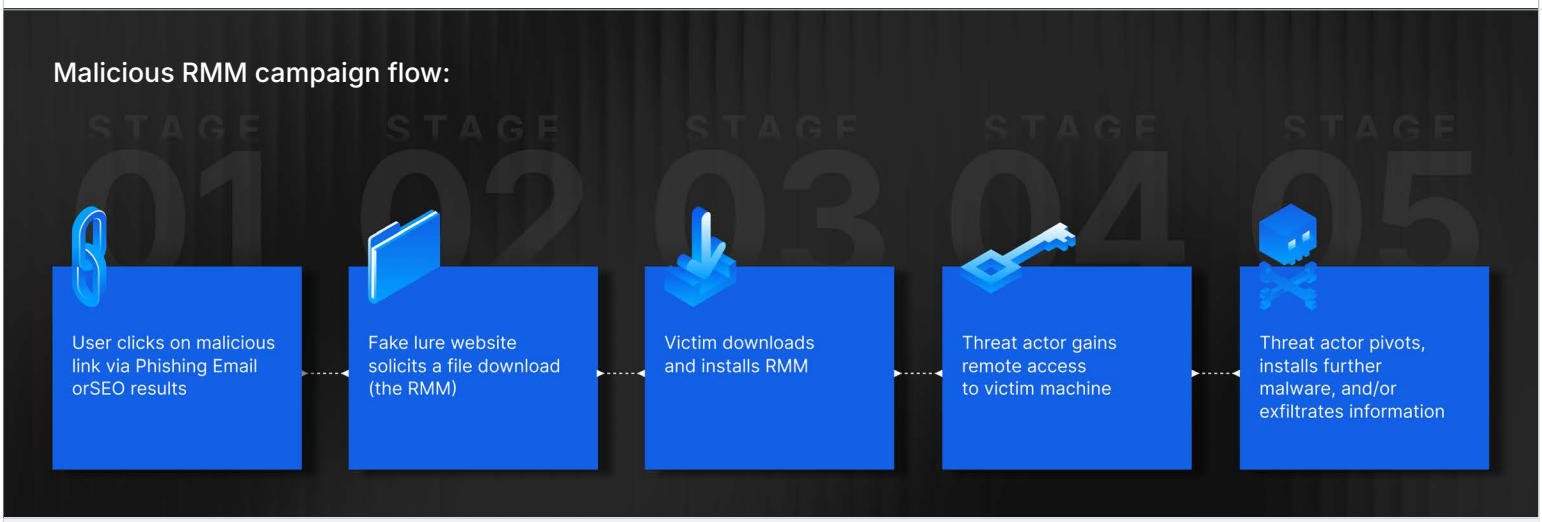
RMM software is incredibly common, used by IT administrators across all sectors to perform tasks like updating and troubleshooting endpoints. RMMs are used to make both endpoints and networks more secure: keeping up to date with patches, troubleshooting routine user errors, and providing convenient remote access to IT teams.

On the flip side, RMMs have the same functionality as Remote Access Trojan (RAT) malware: escalated privileges, screen capture and recording, remote file downloads, remote command line access, and data exfiltration.

At their core, RMMs provide access to a machine the same way RATs do. An attacker may use a RAT to download additional malware or exfiltrate passwords and sensitive information from a machine, whereas an IT administrator uses an RMM to download software or pull error logs from a machine during troubleshooting.

Legacy security solutions apply rigid policies to problems that require contextual analysis. Some classify all RMMs as malicious and automatically remove it from endpoints, disrupting legitimate IT administration and reducing the organization's ability to patch, monitor, and secure systems effectively. Others treat all RMM activity as benign, allowing attackers to abuse legitimate remote access tools for persistence, lateral movement, and data exfiltration without detection. In both cases, the lack of context increases organizational risk rather than reducing it.

Defending against the malicious use of RMMs requires context. Awareness of RMM downloads that come from non-vendor infrastructure is key. Many threat actors use copies of legitimate and licensed RMM software on infrastructure that isn't the original vendor and serve them to victims using fake lure websites in phishing and SEO campaigns.



Technical Details

Most RMM attacks that Trinity Cyber has prevented within the past year come from phishing emails. These emails come in many flavors and themes, but always illicit action from victims. Click this link. Download this invoice. Pay this invoice using a special program. The list goes on.

This section highlights several of the most common RMM campaigns — from initial access to delivery.

Campaign 1: The Secure File

An email hits the inbox with a PDF attachment. A seemingly real purchase order blurred with a fake Microsoft logo with a button to access a "secure file." Purchase order phishing emails are common, as they are meant to mimic normal traffic and often non-technical employees with corporate purchase authority. Clicking the link in the phishing document redirects the user to download a SCR (screensaver) file, which ends up delivering SimpleHelp RMM[1] that's packaged with JWrapper — a method concealing Java source code that also evades detection.

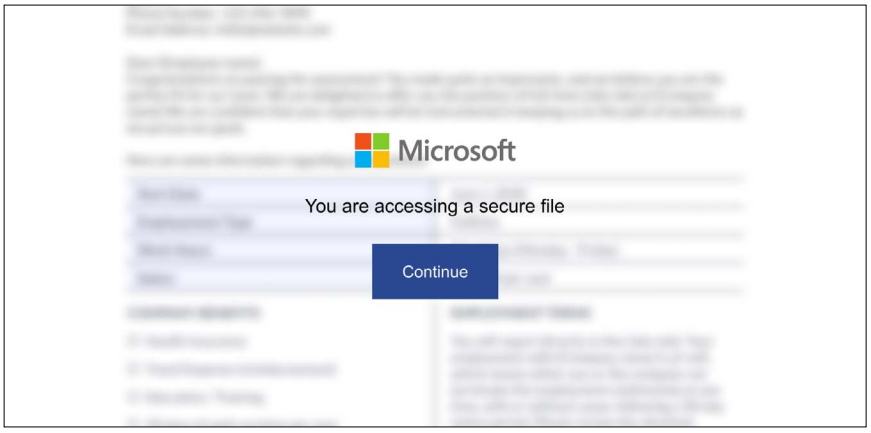


Figure 1. Phishing page for Microsoft "Secure File" download delivering SimpleHelp RMM

SimpleHelp is an RMM enabling full remote access to an endpoint across all major mobile and desktop operating systems. It supports file transfers, remote screen viewing and custom scripting for automation. These are phenomenal capabilities for IT administrators — and for attackers.

The secure file campaign is targeted at employees with purchase authority, often management and executive leadership who have responsibility for paying vendors. By clicking on an otherwise benign-looking purchase order, they download and install an RMM that can be used to pivot throughout the network, exfiltrate sensitive data, and download additional malware within minutes of installation.

Because RMMs are generally viewed as benign or trusted processes, network defenders often overlook them in logs, enterprise security solutions often don't alert on them, and most security teams don't think to look for them. This means threat actors using RMM solutions can take advantage of longer dwell times before defenders recognize their activity.

Campaign 2: The Meeting Transcript

An email hits the inbox claiming there's a meeting transcript from a recent Teams meeting that was held between targets of the phish. An ET Ducky RMM download hides behind a Microsoft Teams-themed lure to download meeting transcripts. ET Ducky is an RMM[2] that specifically advertises the ability for IT administrators to use artificial intelligence to observe Windows Event Tracing for Windows (ETW) logs from the Windows kernel[3]. As part of its troubleshooting suite, ET Ducky allows for live, interactive execution of PowerShell and Windows batch scripts as well as bidirectional file transfers. ET Ducky also has remote desktop capabilities that are valuable to attackers.

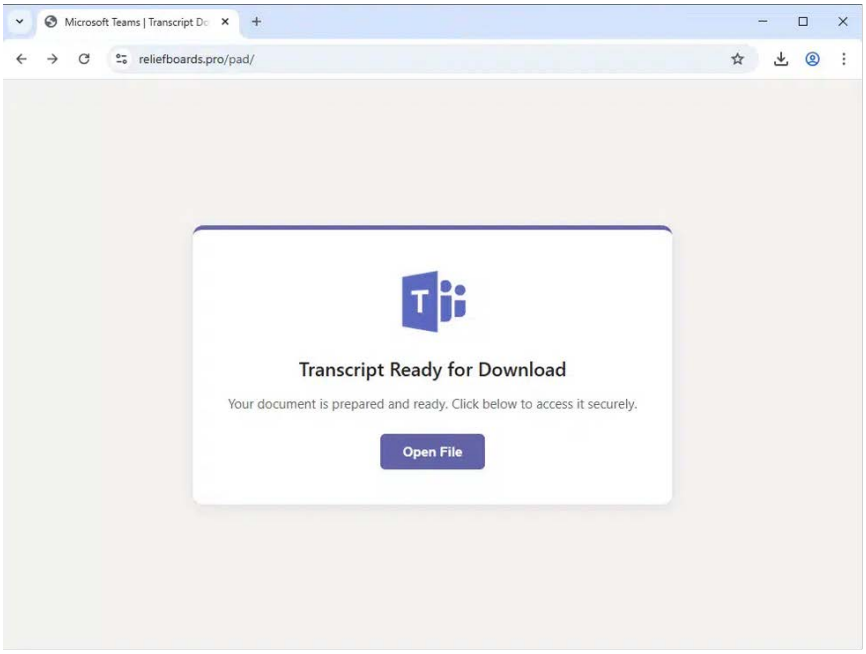


Figure 2. Fake Microsoft Teams transcript delivering ETDucky RMM

Campaign 3: The Software Update

A user is concerned about update messages they're seeing in Adobe Reader. They Google search "Adobe Update" and are presented with some sponsored results to download the latest version of Adobe Reader (plus some standard add-ons). Behind the lure page, Datto RMM[4] hides — ready to be installed by the user. Updates are usually controlled by the IT department, but they're always slammed, and the user doesn't want to bother them. They're just trying to get Adobe Reader updated so they can finish a pressing task.

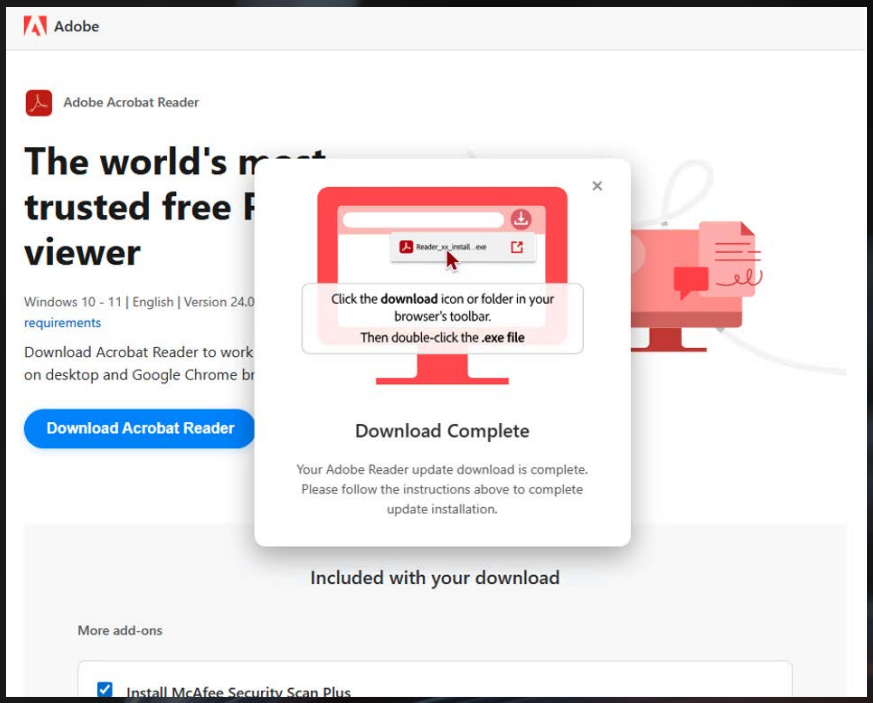


Figure 3. Fake Adobe Reader update delivering Datto RMM

Adding to the complexity, the Adobe download page uses a script that is likely AI-generated, designed to detect bots or security researchers using automated security tools to fetch and analyze campaign artifacts. But this page lets the victim through without any warning, because they're a real person. The bot detection logic is as follows:

```
// AI ANTI-BOT DETECTION SYSTEM (DISTINGUISHES REAL PCs FROM SERVERS)
function detectBot() {
    let score = 0;
    const userAgent = navigator.userAgent.toLowerCase();
    const platform = navigator.platform.toLowerCase();

    console.log('... AI Bot Detection Analysis:');
    console.log('User Agent:', userAgent);
    console.log('Platform:', platform);

    // OPERATING SYSTEM SCORING (60 points max)
    const isWindows = platform.includes('win') || userAgent.includes('windows') || userAgent.includes('win32') || userAgent.includes('win64');
    const isMac = platform.includes('mac') || userAgent.includes('macos') || userAgent.includes('darwin');

    if (isWindows) {
        score += 60;
        console.log('... Windows OS detected: +60 points');
    } else if (isMac) {
        score += 60;
        console.log('... Mac OS detected: +60 points');
    } else {
        score += 5; // Very low score for unwanted OS
        console.log('... Unsupported OS detected: +5 points');
    }

    // REAL PC vs SERVER DETECTION (25 points max)
    // Check for desktop browser indicators
    const hasDesktopFeatures = window.screen && window.screen.width >= 1024 &&
        window.screen.height >= 768 &&
        typeof window.orientation === 'undefined';

    const hasRealBrowserFeatures = navigator.cookieEnabled &&
        navigator.javaEnabled &&
        window.localStorage &&
        window.sessionStorage;

    if (hasDesktopFeatures && hasRealBrowserFeatures) {
        score += 25;
        console.log('... Real desktop PC features detected: +25 points');
    } else {
        score += 2;
        console.log('... Server/headless environment detected: +2 points');
    }
```

Figure 4. Anti-bot source code (AI generated) on Adobe Reader phishing page

Upon installation, the RMM connects to legitimate Datto (a Kaseya company) infrastructure with some unique identifiers to this campaign:

- `vidalcc[.]centrastage[.]net` (Datto US East Web Interface)[5]
- `vid68f60001` (Account Uid)
- `9d39020b-1132-409a-8e67-aeb6550e4f41` (Profile Identifier)

The Kaseya domain is legitimate, and this highlights one of the difficulties in determining malicious vs benign RMM usage on corporate networks. A screenshot of the Datto RMM's custom configuration is shown.

```
<setting name="Profile" serializeAs="String">
  <value>9d39020b-1132-409a-8e67-aeb6550e4f41</value>
</setting>

<setting name="ReceiveTimeout" serializeAs="String">
  <value>60000</value>
</setting>
<setting name="SendTimeout" serializeAs="String">
  <value>60000</value>
</setting>
<!--0 = None-->
<!--1 = Socks4-->
<!--2 = Socks5-->
<!--3 = Http-->
<setting name="ProxyType" serializeAs="String">
  <value>0</value>
</setting>
<setting name="ProxyIp" serializeAs="String">
  <value/>
</setting>
<setting name="ProxyPort" serializeAs="String">
  <value/>
</setting>
<setting name="ProxyUsername" serializeAs="String">
  <value/>
</setting>
<setting name="ProxyPassword" serializeAs="String">
  <value/>
</setting>
<setting name="AccountUid" serializeAs="String">
  <value>vid68f60001</value>
</setting>
</CentraStage.Cag.Core.AppSettings>
```

Figure 5. Datto RMM (formerly CentraStage) configuration used in Adobe campaign

Campaign 4: The Exclusives

Another set of emails hit the inbox. This time, they're invites to parties and social gatherings. Remote work is everywhere, so the user thinks nothing of accepting it. A ScreenConnect[6] RMM download hides behind the invitation to this exclusive social event.

In this campaign, ScreenConnect is packaged alongside a customized configuration file inside a windows MSI file. The victim is presented the phishing site.

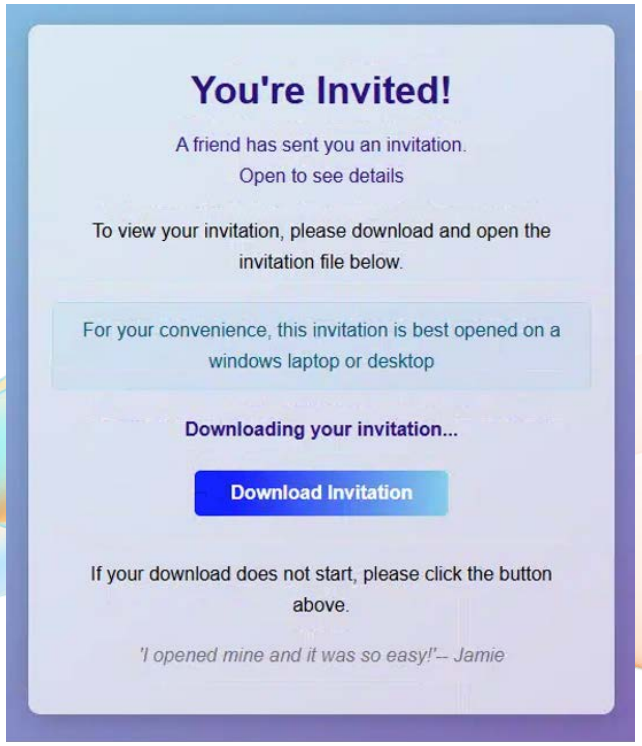


Figure 6. Fake invite page delivering ScreenConnect RMM

When the user clicks download invitation, they download the ScreenConnect RMM in the form of an MSI file which also contains a configuration file, pictured below:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <configSections>
        <section name="ScreenConnect.ApplicationSettings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    </configSections>
    <ScreenConnect.ApplicationSettings>
        <setting name="ClientLaunchParametersConstraint" serializeAs="String">
            <value>?h=instance-rb5vh1-
relay.screenconnect.com&amp;p=443&amp;k=BgIAAACkAABSU0ExAAgAAAEAAQDBsbZGbV4MeyrMWe%2fr8cRkPFYlTctdhvXTLcJHruL2KVI1nc9bNkr%2fg0lS4ObOVZzDxe4z5vY9zNh3T0ciU7bjBKY2qGI2SKYmoYt5GH8FXZ%2bYVuCn
IkutndmJ7%2bFN5LNiTYvcQkoie1xYFnVHLNMLcL0AypaFFQ2b%2bgalfQra%2bQ5ePuA5Wzw3ODgaG3LN5Y0wWb%2f2%2f0HjZIjLfgAoFBsqnC7iEznvrvPWK2%2bloI8lL0NlAFMaMkZyCEHih7uqv%2f2n5tHhuBu%2b6jc1lEa4%2bxX%2f3L
NpJxuSZ49LdmqJ%2fKgBhQtwY5GCJ%2f1qacV9%2bOK1IH9WV2rGfEL1Kdppp3APdRPB</value>
        </setting>
    </ScreenConnect.ApplicationSettings>
</configuration>
```

Figure 7. ScreenConnect XML configuration file within MSI installer

This time, an exclusive eCard comes through. Hiding behind the download button is iTarian RMM, which can automatically patch machines to ensure security compliance, but also enables advanced remote features like other RMMs[7]. This iTarian download is also packaged in an MSI file, hindering it's detection by legacy systems. The phishing page looks like this.

When executed, this iTarian RMM reaches out to custom AWS infrastructure for further instructions. The attacker has full control of the victim's machine.

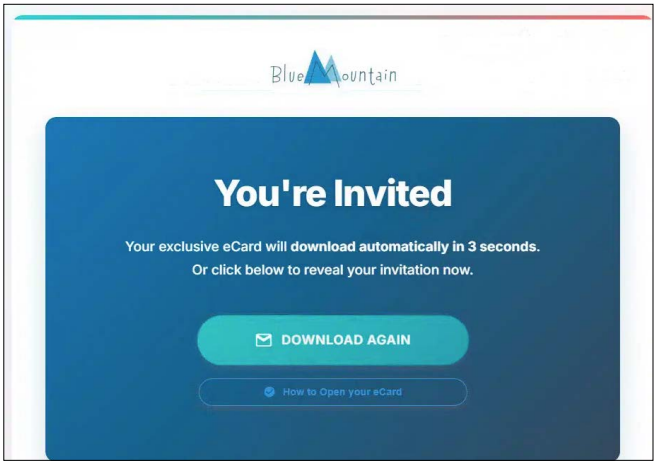


Figure 8. An eCard phishing page delivering iTarian RMM

Campaign 5: The Paperless Post

Similarly, another invite to a party (unclear what type of party)comes through. This attack uses a lesser-known RMM hiding behind the download button. This campaign uses Paperless Post, a legitimate invitation service that's often abused by malicious actors. Once the email is clicked on, the following page is displayed to the user, which ends with a NinjaRMM[8] download.

This campaign involves the use of MSI files to hide and deliver NinjaRMM, configured to reach out to **`agent-us2[.]us2[.]ninjarmm[.]com`** for further instructions. The use of Paperless Post is a known problem, and the vendor has issued guidance for abuse of their platform[9].

The Bigger (RMM) Picture

In modern RMM attacks, threat actors use a wide range – beyond the few examples covered in this analysis. NinjaOne, Datto, ScreenConnect, iTarian, and ET Ducky are just the tip of the iceberg. Some threat actors even use Free and Open Source (FOSS) RMM tools that are obscure and hard to recognize. FOSS RMM tools have the added benefit of being easily customizable — meaning threat actors can change the source code of these tools to add obfuscation, new functionality, or new communication protocols. By now, most RMMs are well categorized by the security community in the LOLRMM project[10]. Yet, many of them fly under the radar due to lack of context around their delivery.

In short, RMMs will continue being popular with attackers: because they blend into your environment and business operations.

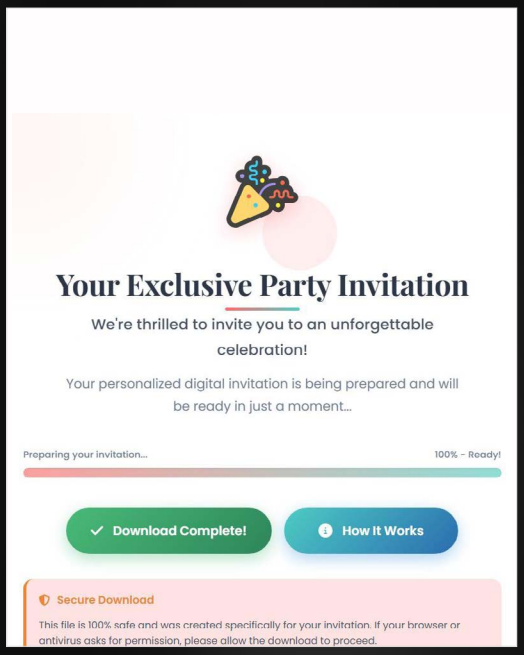


Figure 9. Fake party invite delivering NinjaRMM

How to Stop Malicious RMMs

Trinity Cyber's platform takes a unique approach to threat mitigation for grey area threats like RMMs: collaborate with customers to decide what (if any) RMMs are allowedon their network and remove everything else before it can be delivered to victims. This is more than just whitelisting — it means knowing the full context of a network session around the RMM, including where it came from, where it's supposed to come from, and what (if any) custom configurations are included in the RMM binary within a session.

FCI doesn't play the whack-a-mole hash game. IOCs are artifacts that threat actors leave behind, and Trinity Cyber has moved past them. RMMs and the sessions they are delivered in contain a wide variety of Tactics, Techniques, and Procedures (TTPs) as well as artifacts that are consistent across malicious RMM campaigns.

For many years, organizations have been warning about the use of RMMs in malicious ways. A 2023 CISA report[11] detailed a financially motivated RMM campaign utilizing ScreenConnect that targeted two separate Federal Civilian Executive Branch (FCEB) agencies. The problem has grown extensively since then — and Trinity Cyber's approach stops that problem for customers.

Context for every network session, with a broader view of how RMMs are delivered in malicious campaigns is key to stopping these threats. With FCI in place, organizations operate safely, with no network disruptions, no frustration or friction for their IT departments, and most importantly: threat actors that fail to cause chaos with RMMs.

References

1. https://thehackernews.com/2026/05/phishing-campaign-hits-80-orgs-using.html
2. https://etducky.com
3. https://learn.microsoft.com/en-us/windows/win32/etw/about-event-tracing
4. https://www.datto.com/products/rmm/
5. https://screenconnect.com/integrations/connectwise-rmm/
6. https://rmm.datto.com/help/en/Content/1INTRODUCTION/Requirements/AllowListRequirements.htm?Highlight=allowlist
7. https://itarian.com
8. https://ninjaone.com
9. https://paperlesspost.zendesk.com/hc/en-us/articles/360049322272-Spotting-fake-Paperless-Post-emails-and-spam-texts-How-to-know-what-s-real
10. https://lolrmm.io
11. https://cisa.gov/news-events/cybersecurity-advisories/aa23-025a

IOC	CAMPAIGN	TYPE	PAYLOAD
eb1c09894f15c30c418724984a97d88fe278c87633cf536eeebfa30a5bb85e8c	1	SHA256	SimpleHelp Phishing PDF
longhungphatlogistics[.]vn/quotation/Purchase-Order-list[.]scr	1	URL	SimpleHelp RMM Loader
reliefboards[.]pro/pad/	2	URL	ET Ducky Phishing Page
reliefboards[.]pro/pad/download_invites[.]php	2	URL	ET Ducky RMM
yrnj1m[.]com/Hello/windows_download[.]php	2	URL	iTarian Phishing Page
get-updates[.]org/Adb/invite[.]php	3	URL	Datto RMM Phishing Page
get-updates[.]org/Adb/D%20File	3	URL	Datto RMM
pomu[.]click/ado/gradient[.]html	4	URL	ScreenConnect RMM Phishing Page
pomu[.]click/ado/invite[.]msi	4	URL	ScreenConnect RMM
ytnj1m[.]com/Hello/windows_download[.]php	4	URL	iTarian RMM Phishing Page
myrsvpforme[.]com/Windows/invite[.]php	5	URL	NinjaOne RMM Phishing Page