Spike in Malicious Usage of Screen Connect Software

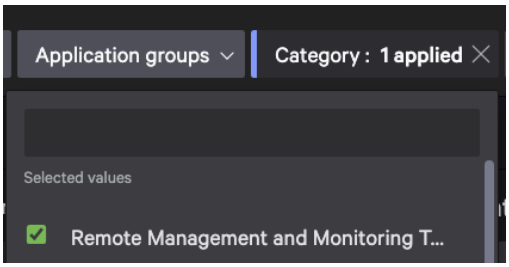
Hello, MCNC and CrowdStrike have seen an uptick in malicious usage of the legitimate software **Screen Connect.** This software is used to facilitate remote access to computers and permits the administrator or bad actor to have control over the computer.

This attack is commonly executed when the user runs an installer script that facilitates the Screen Connect connection or as part of a scareware pop-up where the user calls a number presented, installs the Screen Connect software, and grants the bad actor access to their computer. MCNC has also seen instances of user information compromise, such as sensitive personal information, as part of these attacks.

The best protection against these types of attacks is user awareness training. MCNC recommends reminding your users of these types of attacks, the damage they can cause, and the importance of safe browsing habits. The attached template may be referenced for what such communication would look like.

If you have CrowdStrike in your environment, you can use the Falcon Discover module to show installed and executed applications that match the "Remote Management and Monitoring Tool (RMM Tool)" classification to view the prevalence of Screen Connect, TightVNC, TeamViewer, and other similar software in your environment. If you do not expect to see this software in your environment, you can find the hosts running this software and take action as you see fit. You can access this information by:

1. Log into CrowdStrike
2. Click the hamburger menu in the upper-left corner
3. Exposure Management > Applications > Applications
4. Under the Category heading, choose "Remote Management and Monitoring Tool"



5. You can then adjust the grouping from Application to Managed host by username or by clicking on the hyperlinks the CrowdStrike console presents you for more detailed information.

If you need assistance, please contact secops at secops@mcnc.org or by calling 919-248-4141.

Sample template for engaging your users

Dear [School/Institution Name] Community,

We have been informed of an uptick in malicious software downloads and scareware-style pop-ups. It is crucial that every member of our staff and faculty remains vigilant to avoid unintentional harm to their devices, compromise of personal information, and compromise of our collective digital environment.

How to Protect Yourself:

1. ***Be Skeptical:*** *Do not download files or click on links from unknown sources. Always verify the authenticity of the software through official channels.*
2. ***Use Trusted Networks:*** *Avoid using public or unsecured Wi-Fi to access sensitive information or download files.*

Encountered a Suspicious Link, Pop-Up, or Download?

If you suspect that you have clicked on a suspicious link or accidentally downloaded a questionable file, please take immediate action:

- ***Do Not Proceed****: Refrain from installing or running the file.*
- ***Disconnect from the Network****: This prevents the potential spread of malware.*
- ***Contact IT Help Desk Directly and Immediately****: Our team is here to assist you.*
    - ***Phone:*** *[IT Help Desk Phone Number]*
    - ***Hours:*** *[Available Hours]*

Your timely response is crucial in preventing these threats. By contacting the Help Desk, you enable us to address potential security issues more effectively and protect our community.

Your vigilance is our best defense!

Thank you for taking action to secure your devices and our network.

Best regards,
[Your Name]
[Your Position]
[School/Institution Name]