2025-01-29

HUNTER

EMERGING THREATS

REMOTE MONITORING AND MANAGEMENT (RMM) ABUSE

Remote Monitoring and Management tools have been legitimately used by IT professionals, managed service providers and system administrators to provide the means to monitor and remotely access devices in an effort to streamline the management of IT environments. These tools carry a large amount of power and capability, reducing the need for professionals to be on-site and giving them access to endpoints across the globe. However, these capabilities can be abused and exploited when in a threat actors hands. With organizations more and more relying on RMM tools, malicious actors are able to take advantage and compromise environments masquerading as legitimate software. These tools can give threat actors access to things such as escalated privileges, remote shell access, software deployment, or even move laterally with stolen credentials; all while operating under the radar as a legitimate RMM tool.

THREAT SUMMARY

Remote Monitoring and Management tools have been legitimately used by IT professionals, managed service providers and system administrators to provide the means to monitor and remotely access devices in an effort to streamline the management of IT environments. These tools carry a large amount of power and capability, reducing the need for professionals to be on-site and giving them access to endpoints across the globe. However, these capabilities can be abused and exploited when in a threat actors hands. With organizations more and more relying on RMM tools, malicious actors are able to take advantage and compromise environments masquerading as legitimate software. These tools can give threat actors access to things such as escalated privileges, remote shell access, software deployment, or even move laterally with stolen credentials; all while operating under the radar as a legitimate RMM tool.

This collection is focused on providing Hunt packages to best identify activities related to the installation and abuse of RMM tools. The target scope RMM tools provided in this collection are popular tools, used legitimately in many organizations, therefore analysts should first determine if the tool associated with the Hunt Package is allowed in the organization. If it is allowed by exception, analysis of the results should take this into account.

Intel 471 References:

[Intelligence Bulletin: Rise of remote monitoring, management software]
(https://titan.intel471.com/report/fintel/660167cd88d8249928c27e24f7a43dd9)

SYNOPSIS

This collection of Threat Hunt Packages gives analysts visibility into a number of Remote Monitoring and Management tools that can be abused by malicious actors and malware variants in order to gain initial access, gain remote access and/or maintain persistence in an environment.

[AnyDesk]
AnyDesk is known as a Remote Desktop application developed by AnyDesk Software GmbH, typically utilized legitimately to allow access and control to remote devices, servers, and machines. Unfortunately, threat actors leverage and exploit the collaboration software to gain access to proprietary data by tricking targets into installing the software. Threat actor groups such as Medusa, Rhysida, Mad Liberator, Cactus and Lockbit are among the adversaries observed to exploit the software.

[Atera Agent]
Atera Agent is a software that is considered the core of the Atera monitoring system. It is typically used to be installed on a computer or server, and is utilized legitimately to track system health and diagnostics; it is also can be used for remote patching, deployment and script execution. Threat actors such as MuddyWater (or TA450) have exploited the agent for malicious purposes by installing Atera Agent via .MSI files, and thus gaining unauthorized access to the remote capabilities of the software on the victimâ€™s system.

[Meshagent]
MeshAgent is the endpoint software associated with the open source remote management platform called MeshCentral. When installed, MeshAgent allows the operator to gain access to full remote management of the endpoint, and thus can be exploited by threat actors to gain unauthorized access to a victimâ€™s system. Threat actors such as LilacSquid, Awaken Likho, and Tur0k have been observed to be exploiting this agent to conduct malicious activities that include reconnaissance, data exfiltration and further malware deployment.

[QuickAssist]
Microsoft QuickAssist is a remote assistance software that is natively integrated into Windows, and developed my Microsoft to offer remote troubleshooting and technical support. Due to it being already installed on Windows 10/11 machines, the software has been exploited by a number of threat actors; being utilized via social engineering attacks where operators masquerade as a trusted Microsoft technical professional to gain access. Threat actors such as Black Basta (or Storm-1811Â) and Bezenchuk have been seen exploiting MS QuickAssist in an effort to gain initial access and persistence.

[NetSupport Manager]
NetSupport manager is a long-established Remote Desktop software that was first released in 1989, allowing remote access for IT administrators and professionals in order to provide technical support remotely. Similar to other RMM tools, NetSupport manager has been exploited to be used maliciously, to a point of a malicious by-product of the platform being created - aptly named NetSupport RAT. This spin-off Remote Access Trojan has been used by the infamous financially motivated threat group named FIN7 (or Carbanak), as well as in a number of other campaigns aiming to employ the remote access software capabilities in their attacks.

[ScreenConnect]
Connectwise ScreenConnect is similar to the other Remote Monitoring and Management tools, allowing remote support for endpoints and other hardware for an extensive number of organizations. Unfortunately, due to its common usage, it has been the target of exploitation by threat actors in recent years. Most notably in 2024, there were two critical vulnerabilities discovered that allowed attackers remote code execution capabilities. Threat actors such as Black Basta, LockBit and Bl00dy were observed to exploit these vulnerabilities.

[Splashtop]
Splashtop is another Remote Monitoring and Management tool that is widely used, offering similar remote tooling that can be abused to afflict victims machines. This tooling includes monitoring, remote control access and file sharing capabilities as well. Threat groups such as RansomHub, BianLian and Cactus have been observed to exploit the usage of Splashtop to gain access to victims systems. After exploitation, it has been utilized to maintain persistence on targets and access sold to bidders.

[TeamViewer]
Developed by TeamViewer SE, TeamViewer is a widely known Remote Monitoring and Management software that has been used since 2005. Offering similar capabilities as other RMM tools, TeamViewer allows an operator connection to a device regardless of operating system. Unfortunately, just like the other tools, the software has been used maliciously to gain initial access into organizations - notably TeamViewer was observed to be used alongside the deployment of LockBit 3.0 ransomware in 2024.

HUNT PACKAGES

SUSPICIOUS CHILD PROCESS FOR SCREENCONNECT - POTENTIAL EXPLOITATION ACTIVITY
https://hunter.cyborgsecurity.io/research/hunt-package/2cac1faf-2e44-4c12-a7b3-fa2756902691

SCREENCONNECT SERVICE INSTALL - POTENTIALLY MALICIOUS RMM TOOL INSTALLATION https://hunter.cyborgsecurity.io/research/hunt-package/

SPLASHTOP RMM COMMAND LINE INSTALL https://hunter.cyborgsecurity.io/research/hunt-package/d6ea6636-943e-4232-afb7-c67c5ec1c999

SCREENCONNECT EXECUTION FROM ABNORMAL FOLDER - POTENTIAL MALICIOUS USE OF RMM TOOL
https://hunter.cyborgsecurity.io/research/hunt-package/

NETSUPPORT MANAGER EXECUTION FROM ABNORMAL FOLDER - POTENTIAL MALICIOUS USE OF RMM TOOL

https://hunter.cyborgsecurity.io/research/hunt-package/3F329A8C-0102-4A61-8CF3-63948AAB5EF4 **MESHAGENT**

SERVICE INSTALLATION https://hunter.cyborgsecurity.io/research/hunt-package/30BD6983-BAC4-4645-AB55-

68E52F11B5F5

POTENTIAL SCREENCONNECT RELAY MODE ACTIVITY https://hunter.cyborgsecurity.io/research/hunt-package/f5d9bda0-a982-485e-94f7-701352850fad

MESHAGENT SUSPICIOUS CHILD PROCESS - POTENTIAL MALICIOUS RMM TOOL USAGE
https://hunter.cyborgsecurity.io/research/hunt-package/749F7E2C-5EEB-407D-A5EF-CFCECBE5D810

ATERA AGENT UTILIZED FOR UNAUTHORIZED REMOTE ACCESS https://hunter.cyborgsecurity.io/research/hunt-package/b479f6b2-b14c-4667-be40-6ec310dbd934

ANYDESK SILENT INSTALLATION - POTENTIAL MALICIOUS RMM TOOL INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/11353A3B-797D-45BC-BA32-3D10F14EDC82

REMOTE ATERA AGENT DOWNLOAD - COMMAND LINE https://hunter.cyborgsecurity.io/research/hunt-package/bb771c73-e7ab-4705-92a2-ce322b33621d

REMOTE ATERA AGENT DOWNLOAD - WEB https://hunter.cyborgsecurity.io/research/hunt-package/7ccc1404-1499-45ba-9c7d-59f42ba321e3

ANYDESK PASSWORD SET VIA CLI - POTENTIAL MALICIOUS RMM TOOL INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/8E0CF375-A8D7-46BD-B9B9-C7181B194706

ANYDESK SERVICE INSTALLATION - POTENTIALLY MALICIOUS RMM TOOL INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/4103B086-F093-4084-9125-15B9A6C872B8

CUSTOM SERVICE OR INSTALLATION FOR MESHAGENT - POTENTIAL MALICIOUS RMM TOOL INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/FD4C499E-CF30-4001-BB30-438088AD4880 **NETSUPPORT MANAGER SERVICE INSTALL - POTENTIALLY MALICIOUS RMM TOOL INSTALLATION**
https://hunter.cyborgsecurity.io/research/hunt-package/2C51DE08-F4B6-4952-B42B-3C27628ECC99

QUICK ASSIST CONFIGURATION DIRECTORY CREATION - POTENTIALLY MALICIOUS RMM TOOL USAGE

https://hunter.cyborgsecurity.io/research/hunt-package/A8F60A2E-34BC-4BDE-8554-C8CB8FD4CE7B **ANYDESK**

EXECUTION FROM ABNORMAL FOLDER - POTENTIAL MALICIOUS USE OF RMM TOOL

https://hunter.cyborgsecurity.io/research/hunt-package/93F71607-F35D-4AA6-AEC9-C2F8A62CBD8A

RELATED LINKS

Sign up for free HUNTER access
Remote Monitoring and Management (RMM) Abuse Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Command and Control
- Technique Names:
  - Remote Access Software
- Threat Names:
  - RansomHub Ransomware
  - Rhysida
  - Emotet
  - IcedID
  - Modiloader
  - Hive Ransomware
  - QakBot
  - BlackBasta Ransomware

REFERENCES

1. https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/
2. https://thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/
3. https://blog.talosintelligence.com/lilacsquid/
4. https://titan.intel471.com/report/fintel/660167cd88d8249928c27e24f7a43dd9
5. https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/
6. https://github.com/AiGptCode/ANYDESK-BACKDOOR/blob/main/Anydesk-backdoor(Admin).py
7. https://support.anydesk.com/knowledge/installation
8. https://support.anydesk.com/Automatic_Deployment
9. https://meshcentral.com/tools/
10. https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/
11. https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
12. https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware/
13. https://www.advintel.io/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent
14. https://security.microsoft.com/threatanalytics3/18643500-71c7-433a-806b1b8649f83f15/analystreport/vulnerability
15. https://redcanary.com/blog/threat-detection/misbehaving-rats/
16. https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7threat-actor/

17. https://thedfirreport.com/2024/04/01/from-onenote-to-ransomnote-an-ice-cold-intrusion/
18. https://thedfirreport.com/2022/06/16/sans-ransomware-summit-2022-can-you-detect-this/
19. https://thedfirreport.com/2023/09/25/from-screenconnect-to-hive-ransomware-in-61-hours/
20. https://support-splashtoponprem.splashtop.com/hc/en-us/articles/900000428026-Command-line-parameters-tosilently-install-your-Splashtop-Streamer-and-Client-app
21. https://www.nccgroup.com/us/research-blog/the-dark-side-how-threat-actors-leverage-anydesk-for-maliciousactivities/
22. https://www.sygnia.co/blog/luna-moth-false-subscription-scams/
23. https://github.com/Ylianst/MeshAgent/blob/master/readme.md
24. https://resources.netsupportsoftware.com/resources/whitepapers/NetSupport%20Manager%20Global%20client32.ini%20files.pdf
25. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a