State of the Remote Access Tools, Part 1

medium.com/walmartglobaltech/state-of-the-rat-part-1-cfec6c967e2f

Jason Reaves

August 19, 2022

Jason Reaves

Aug 11

·

6 min read

By: Zori Bennett

Remote Access Tools (RATs) are software that allow users to gain access to their computer system remotely from another location. Some key features with these tools include file sharing, cloud storage, video/text chat capabilities, etc. Although it can be deemed genuine for a commercial user, threat actors can utilize these systems to carry out malicious attacks and steal data. In this report, the following commonly exploited remote access tools used by malicious actors will be focused on: RemotePC, Ultraviewer, MSP360, PDQDeploy, and ZohoAssist.

RemotePC

RemotePC is a free commercial tool created by iDrive Inc. that allows users to remotely access and control their Windows, Mac, or Linux computers from other devices. Features with the software include messaging tools, file transfer and multiple monitor support. Currently there have been confidential reports stating its relevance and usage in threat actor breaches.

Vulnerability Reports/CVE

The most recent vulnerability reports on RemotePC were taken in July of 2022 (CVE-2021–34688 and CVE-2021–34687)[7]. Previous versions allowed for several security threats such as denial of service, authentication bypasses, privilege escalation, information disclosure and man-in-the-middle attacks.

Verified Signer(s):

```
iDrive Inc.ProSoftnet Corporation
```

Associated File Names:

```
RemotePCRPC DND ConsoleRemotePCServiceRemotePC SuiteRPC Performance
ServiceRpcOTADND_Console.exeRemotepcservice.exeRemotePCUIU.exeRPCPerformanceService.ex
```

Associated Domains:

```
version.remotepc[.]comweb1.remotepc[.]comwww1.remotepc[.]com
```

Associated IPs:

```
172.67.37.12364.90.202.20064.90.202.245
```

Associated Hashes:

```
8e6357da8f7666f608b38c36aacca109348ada83cf10179dd253d90d04fdbf1e9c1c06d4cd5e02f306bd4f
```

Under normal circumstances, RemotePC typically executes from these paths:

```
%SAMPLEPATH%\RemotePC.exe%USERPROFILE%\AppData\Local\Temp\is-
VHFM6.tmp\RemotePC.tmp%USERPROFILE%\AppData\Local\Temp\is-
KO4JJ.tmp\RemotePC1.exe%USERPROFILE%\AppData\Local\Temp\is-
UG36L.tmp\RemotePC1.tmpC:\Windows\SysWOW64\taskkill.exeC:\Program Files
(x86)\RemotePC\RPDUILaunch.exeC:\Program Files
(x86)\RemotePC\PreUninstall.exeC:\Program Files
(x86)\RemotePC\RPCFirewall.exeC:\Program Files
(x86)\RemotePC\SuiteLauncher.exeC:\Program Files
(x86)\RemotePC\RemotePCLauncher.exeC:\Windows\SysWOW64\sc.exeC:\Windows\System32\msiex
 Files (x86)\RemotePC\RPCDownloader.exeC:\Program Files
(x86)\RemotePC\RemotePCService.exeC:\Program Files
(x86)\RemotePC\RPCPrinterDownloader.exeC:\Windows\System32\cmd.exeC:\Windows\System32\
 Files
(x86)\RemotePC\RemotePCUIU.exeC:\ProgramData\RemotePC\Codec\RemotePCPerformance.exeC:\
 Files (x86)\RemotePC\RemotePCPerformance\RPCPerformanceService.exeC:\Program Files
(x86)\RemotePC\RemotePCPerformance\RpcApp\Tools\RpcUtility.exeC:\Windows\System32\regs
 Files (x86)\RemotePC\RemotePCPerformance\PluginInstaller.exeC:\Program Files
(x86)\RemotePC\RemotePCPerformance\RemotePCPerformancePlugins.exeC:\Program Files
(x86)\RemotePC\RemotePCPerformance\RemotePCPerformancePrinter.exeC:\Program Files
(x86)\RemotePC\RemotePCPerformance\RpcPrinter\InstallPrinter.exe%SAMPLEPATH%\3d11cf1d5
G102D.tmp\3d11cf1d5f83678258e790b34e99f5c71c2dc3f14a27dd5f14192ab10b4d0217.tmp%USERPRO
H2LAQ.tmp\RemotePC1.exe%USERPROFILE%\AppData\Local\Temp\is-
K8CKA.tmp\RemotePC1.tmp"C:\Windows\system32\rundll32.exe"
C:\Windows\system32\shell32.dll,OpenAs_RunDLL C:\Program
Files\RemotePC\rootcert.pem"C:\Windows\System32\msiexec.exe" /qn /i
"C:\ProgramData\RemotePC\PrinterSetup\Printer.msi"
```

Ultraviewer

Ultraviewer, signed by DucFabulous Co., Ltd, is a tool with various capabilities including support on all versions of Windows, chat boxes and remote file sharing.

One of the latest occurrences of a threat actor utilizing Ultraviewer is its feature detected by AT&T Alien Labs in a remote access trojan called ‘FatalRAT’[1]. The malware allowed for attackers to run tests that checked for virtual machines within the system before executing commands to infect the system remotely. A key factor of this malware was that it actively uninstalled Ultraviewer and installed AnyDesk. Under suspected circumstances, the malware will spread on the victim’s network by brute-forcing weak passwords through IPC$. If successful, the malware copies itself to the dedicated folder as %Folder%\hackshen.exe and will execute the copied file remotely.

Another usage of UltraViewer was as a tool in an exam hacking scheme, Delhi Police arrested three Russian hackers who were hired to supply answers for various reputable exams (e.g. GMAT, IBM, CCISO, etc.)[2]. The hackers claimed to have helped hundreds of candidates and have been ongoing since 2019. On exam day, the hackers would send a link to the ‘Ultraviewer’ software for their clients to download. From there, the clients would use Ultraviewer to grant access to the hacker who inputs the correct answers to the test.

Verified Signer(s):

```
DucFabulous Co., Ltd
```

Associated File Names:

```
UltraViewerDesktopUltraViewerServiceUltraViewer_Service.exeis-
AQ77Q.tmpUltraViewer_Desktop.exeis-273TE.tmp
```

Associated IPs:

```
20.99.132.105:443 (TCP)91.199.212.52:80 (TCP)172.64.155.188:80 (TCP)104.18.32.68:80
(TCP)23.216.147.64:443 (TCP)13.107.4.50:80 (TCP)192.168.0.1:137
(UDP)23.216.147.76:443 (TCP)
```

Associated Hashes:

```
e18e537dd5869f41e09eee5e598a6fb0817f79b3b7d38d9fdd36015d9f5596ecc92d5dfc09749554afd917
```

Under normal circumstances, Ultraviewer typically executes from these paths:

```
%SAMPLEPATH%\UltraViewer_setup_6.5_en.exe%USERPROFILE%\AppData\Local\Temp\is-
3QM76.tmp\UltraViewer_setup_6.5_en.tmpC:\Windows\System32\wuapihost.exe%SAMPLEPATH%\7d
61CG1.tmp\7db985064e0bf2f94ee071a83f57f8611e06039f0adcced38065deedf621526a.tmp%USERPRO
T02CO.tmp\7db985064e0bf2f94ee071a83f57f8611e06039f0adcced38065deedf621526a.tmp%USERPRO
CQM9G.tmp\7db985064e0bf2f94ee071a83f57f8611e06039f0adcced38065deedf621526a.tmp%USERPRO
6SFKI.tmp\7db985064e0bf2f94ee071a83f57f8611e06039f0adcced38065deedf621526a.tmp%USERPRO
VIO6F.tmp\7db985064e0bf2f94ee071a83f57f8611e06039f0adcced38065deedf621526a.tmp%USERPRO
376TQ.tmp\7db985064e0bf2f94ee071a83f57f8611e06039f0adcced38065deedf621526a.tmp
```

MSP360

MSP360, formerly known as CloudBerry Lab, is a software with not only remote access capabilities, but disaster recovery and backup management. The platform can be used across various operating systems (Windows, MacOS, Linux) and platforms including, VMWare, Google Workspace and Microsoft365. Currently, there have been confidential reports involving the software, msp360[.]com in threat actor breaches.

Verified Signer(s):

```
CloudBerry LabMSPBytes, Corp.Sectigo Public Code Signing CA
```

Associated File Names:

```
MSP
ConnectCloudRaService.exeCloudRaWpf.exeConnect.exeConnectStandaloneSetup_v3.0.0.60_net
```

Associated IPs:

```
13.107.4.52:80 (TCP)52.251.79.25:443 (TCP)23.216.147.76:443 (TCP)
```

Associated Hashes:

```
35c46ce77a20732eac2db689befa652107670df51a96d6de48365765c357901027032e70a9bac6889d4775
```

Registry Keys:

Under normal circumstances, MSP360 typically executes from these paths:

```
%user%\Desktop\CloudBerry Remote Assistant.lnkC:\ProgramData\Microsoft\Windows\Start
Menu\Programs\CloudBerryLab\CloudBerry Remote
Assistant\Uninstall.lnkC:\ProgramData\Microsoft\Windows\Start
Menu\Programs\CloudBerryLab\CloudBerry Remote Assistant\CloudBerryLab Web
Site.lnkC:\ProgramData\CloudBerryLab\CloudBerry Remote Assistant\Logs\CloudBerry
Remote Assistant.logC:\ProgramData\Microsoft\Windows\Start
Menu\Programs\CloudBerryLab\CloudBerry Remote Assistant\CloudBerry Remote
Assistant.lnkC:\Program Files\ConnectC:\Program
Files\Connect\AudioProcessingModuleCs.dllC:\Program
Files\Connect\Cloud.Backup.RM.SIO.dllC:\Program
Files\Connect\Cloud.Base.dllC:\Program Files\Connect\Cloud.Client.dllC:\Program
Files\Connect\Cloud.RA.dllC:\Program Files\Connect\Cloud.Ra.AppConfig.dllC:\Program
Files\Connect\Cloud.Ra.Client.dllC:\Program
Files\Connect\Cloud.Ra.Common.XmlSerializers.dllC:\Program
Files\Connect\Cloud.Ra.Common.dllC:\Program
Files\Connect\Cloud.Ra.CommonHelpers.dllC:\Program
Files\Connect\Cloud.Ra.DirectConnection.dllC:\Program
Files\Connect\Cloud.Ra.FileTransfer.dllC:\Program
Files\Connect\Cloud.Ra.Firewall.dllC:\Program
Files\Connect\Cloud.Ra.Server.dllC:\Program
Files\Connect\Cloud.Ra.ServiceContract.dllC:\Program
Files\Connect\Cloud.Ra.TransportController.dllC:\Program
Files\Connect\Cloud.Ra.Video.dllC:\Program
Files\Connect\Cloud.Ra.WinApi.dllC:\Program Files\Connect\CloudRaCmd.exeC:\Program
Files\Connect\CloudRaCmd.exe.configC:\Program Files\Connect\CloudRaSd.exeC:\Program
Files\Connect\CloudRaSd.exe.configC:\Program
Files\Connect\CloudRaService.InstallLogC:\Program
Files\Connect\CloudRaService.InstallStateC:\Program
Files\Connect\CloudRaService.exeC:\Program
Files\Connect\CloudRaService.exe.configC:\Program
Files\Connect\CloudRaUtilities.exeC:\Program
Files\Connect\CloudRaUtilities.exe.configC:\Program
Files\Connect\Connect.exeC:\Program Files\Connect\Connect.exe.configC:\Program
Files\Connect\ICSharpCode.SharpZipLib.dllC:\Program
Files\Connect\InstallUtil.InstallLogC:\Program Files\Connect\LZ4.dllC:\Program
Files\Connect\MagnifierCapture.dllC:\Program Files\Connect\NAudio.dllC:\Program
Files\Connect\NAudio.xmlC:\Program Files\Connect\Newtonsoft.Json.dllC:\Program
Files\Connect\Open.Nat.dllC:\Program Files\Connect\Open.Nat.xmlC:\Program
Files\Connect\install.logC:\Program Files\Connect\librtc.dllC:\Program
Files\Connect\license.txtC:\Program Files\Connect\mainicon.icoC:\Program
Files\Connect\x86C:\Program
Files\Connect\x86\librtc.dllC:\ProgramData\ConnectC:\ProgramData\Connect\ExternalReque
 Files\CloudBerryLab\CloudBerry Remote Assistant\"
```

PDQ Deploy

PDQ Deploy is a software tool that allows users to create custom deployment packages. Essentially, users can install software remotely on any system.

PDQ Deploy used by threat actors:

A Ransomware-as-a-service (RaaS) software by the name of Avos Locker utilized multiple remote access tools to carry out attacks and exploit vulnerabilities. The attackers were utilizing the safe mode configuration to disable most Windows third party drivers and endpoint security software[3]. Thus Avos Locker attackers were rebooting the machines into Safe Mode and running the IT management tool AnyDesk. The attackers also leverage PDQ Deploy to push out batch scripts to their targeted machines. This in return would carry out their attack in deploying the Avos Locker ransomware.

Verified Signer(s):

```
PDQ.COM Corporation
```

Associated File Names:

```
PDQDeploy SetupPDQDeploy
ServicePDQDeployService.exePDQDeployConsole.exePDQDeploySetup.exePDQDeploy.19.3.310.0.
```

Associated IPs:

```
192.168.0.54:137 (UDP)23.61.187.27:80 (TCP)20.99.132.105:443 (TCP)23.216.147.76:443
(TCP)23.49.139.27:80 (TCP)23.216.147.64:443 (TCP)
```

Associated Hashes:

```
07ccb95db2924e2e2b70dfb2a1275d15d36bbe014390a4a5619557698e3a077a03406847b2d1fb9ce71ac9
```

Under normal circumstances, PDQ Deploy typically executes from these paths:

```
%SAMPLEPATH%\Deploy_19.3.310.0.exeC:\Windows\Downloaded Installations\Admin
Arsenal\PDQ Deploy\19.3.310.0\PDQDeploySetupPrep.exe%SAMPLEPATH%\PDQDeploySetup.exe
```

ZohoAssist

ZohoAssist is a remote access tool that emphasizes initiating and scheduling remote support sessions and troubleshoot issues via the web browser.

ZohoAssist used by threat actors:

Luna Moth Phishing Attack (July 12th, 2022)

The Luna Moth ransom group, also named Silent Ransom Group, have carried out a phishing scam using commercial remote access tools such as Atera, Anydesk, Syncro and Splashtop. The group was recognized by the Incident Response team at Sygnia . Luna Moth’s tactic included luring victims with false subscriptions for Zoho Masterclass or Duolingo.[4] The victim is initially sent a counterfeit invoice to renew a subscription for selected services that were not originally purchased. When prompted to dispute the charge or cancel the subscription, the victim would contact customer service which would be one of the threat actors via phone. The threat actor would then provide instructions to install remote access tools on the victim’s system. Further after receiving access, the threat actor would install other tools such as Rclone, SharpShares and SoftPerfect network Scanner to steal user data.

Zoho ManageEngine Vulnerability Incident (February 16, 2022)

Threat actor that goes by the name, ”unindicted”, exploited a Zoho ManageEngine vulnerability that allowed them to execute code. Without authentication to the International Committee of the Red Cross network.[5] The vulnerability tracked as CVE-2021–40539 allowed the actor to execute privilege escalation and exfiltrate registry hives and active directory files through web shells.

Verified Signer(s):

```
Zoho Corporation Private Limited
```

Associated File Names:

```
Zoho
AssistConnect.exeza_connect.exeZohoURSService.exeZAService.exezaservice.exeZohoAssistZ
```

Associated Domains:

```
downloads.zohocdn.comassist.cs.zohohost.comzohoassist.comzohohost.comassistlab.zoho.cc
```

Associated IPs:

```
136.143.191.95:443 (TCP)136.143.190.0/23
```

Associated Hashes:

```
4f98f565336d5bb142239c4007ec1d9492caf4c31020176de380c8b31c9129edb72f8cb789ebb129640e8f
```

Registry Keys:

```
HKLM\System\CurrentControlSet\Services\Zoho Assist-Remote
SupportHKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Zoho
AssistHKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Zoho
Assist Customer
PluginHKEY_CURRENT_USER\Software\Classes\zohoassistlaunchHKEY_CURRENT_USER\Software\Cl
 Assist-Remote
SupportHKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Zoho
AssistHKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Zoho
Assist Customer
PluginHKEY_CURRENT_USER\Software\Classes\zohoassistlaunchHKEY_CURRENT_USER\Software\Cl
```

Under normal circumstances, Zoho Assist typically executes from these paths:

```
'C:\Program Files (x86)\ZohoMeeting\agent.exe' -agent -k 106052736 -s
gwlabin1.zohoassist.com -altgw gwlab-wa.zohoassist.com -fileTransferGateways ft1-
in1.zohoassist.com -ms assistlab.zoho.com -ssl true -email Arjun -authkey
0tWHPnTrsFAmRLJgEsaMp9Bizvry/FqxYLVMuFpj59nsRLUlmLb+ewcWgZXJiAx3exDxNdyuWDAhFXagn9DnaA
 -authtype 1 -SERVICEAGENT -demo_mode false -demo_tech false -ShowInit 0 -group AUL -
productID 1 -js join.zoho.com -c_check false
```

References

1: https://cybersecurity.att.com/blogs/labs-research/new-sophisticated-rat-in-town-fatalrat-analysis

2: https://indianexpress.com/article/cities/delhi/russian-hackers-jee-gmat-exams-arrested-7708815/

3: https://news.sophos.com/en-us/2021/12/22/avos-locker-remotely-accesses-boxes-even-running-in-safe-mode/

4: https://www.bleepingcomputer.com/news/security/new-luna-moth-hackers-breach-orgs-via-fake-subscription-renewals/

5: https://threatpost.com/zoho-zero-day-manageengine-active-attack/177178/

6: https://www.ultraviewer.net/en/200000026-summary-of-ultraviewer-s-security-information.html

7: https://www.opencve.io/cve?cvss=&search=remotepc