DarkComet: Backdoor.DarkComet

Archived: 2026-04-02 11:01:21 UTC

Short bio

Backdoor.DarkComet is a Remote Access Trojan (RAT) application that may run in the background and silently collect information about the system, connected users, and network activity.Backdoor.DarkComet may attempt to steal stored credentials, usernames and passwords, and other personal and confidential information. This information may be transmitted to a destination specified by the author.Backdoor.DarkComet may also allow an attacker to install additional software to the infected machine, or may direct the infected machine to participate in a malicious botnet for the purposes of sending spam or other malicious activities.

Symptoms

Backdoor.DarkComet may run silently in the background and may not provide any indication of infection to the user. Backdoor.DarkComet may also disable antivirus programs and other Microsoft Windows security features.

Type and source of infection

Backdoor.DarkComet may be distributed using various methods. This software may be packaged with free online software, or could be disguised as a harmless program and distributed by email. Alternatively, this software may be installed by websites using software vulnerabilities. Infections that occur in this manner are usually silent and happen without user knowledge or consent.

Protection

Malwarebytes protects users from the installation of Backdoor.DarkComet. Malwarebytes detects and removes Backdoor.DarkComet

Home remediation

Malwarebytes can detect and remove many Backdoor.DarkComet infections without further user interaction.

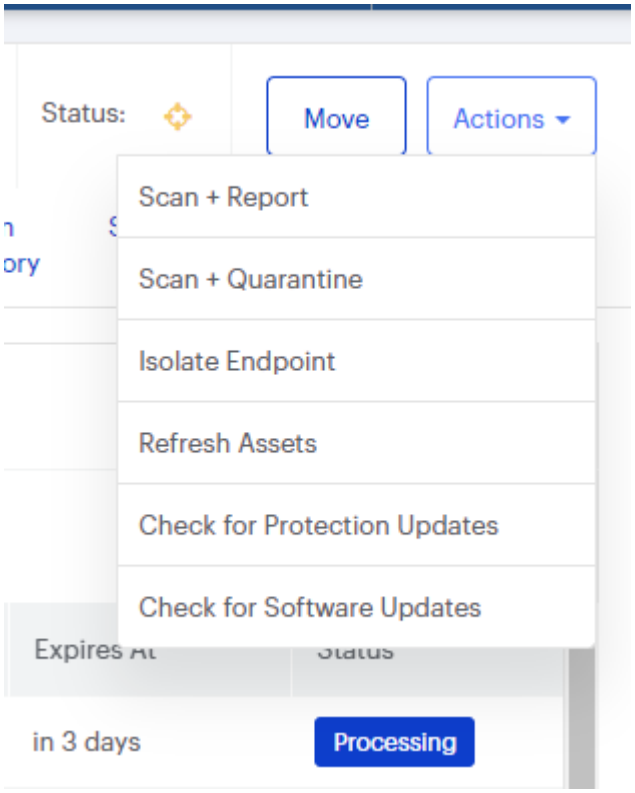
1. Please download Malwarebytesto your desktop.
2. Double-click **MBSetup.exe**and follow the prompts to install the program.
3. When your **Malwarebytes for Windows**installation completes, the program opens to the Welcome to Malwarebytes screen.
4. Click on the **Get started** button.
5. Click **Scan** to start a **Threat Scan**.
6. Click **Quarantine**to remove the found threats.

7. Reboot the system if prompted to complete the removal process.

Business remediation

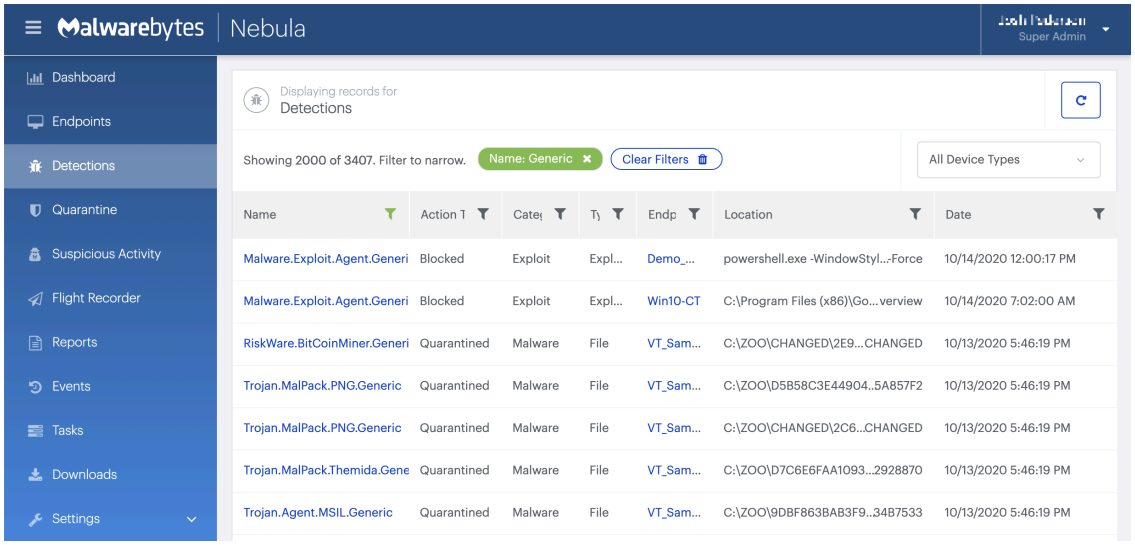
How to remove Backdoor.DarkComet with the Malwarebytes Nebula console

You can use the Malwarebytes Anti-Malware Nebula console to scan endpoints.

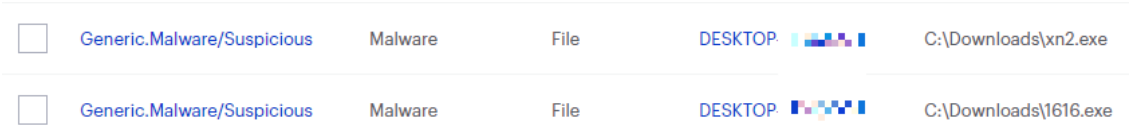


Nebula endpoint tasks menu

Choose the Scan + Quarantine option. Afterwards you can check the Detections pageto see which threats were found.



On the Quarantine pageyou can see which threats were quarantined and restore them if necessary.



Malwarebytes removal log

A Malwarebytes log of removal will look similar to this: Malwarebyteswww.malwarebytes.com-Log Details-Scan Date: 3/21/18Scan Time: 10:22 PMLog File: 92c470fc-2d88-11e8-afe9-00ffc8517b86.jsonAdministrator: Yes-Software Information-Version: 3.4.4.2398Components Version: 1.0.322Update Package Version: 1.0.4442License: Premium-System Information-OS: Windows 7 Service Pack 1CPU: x64File System: NTFSUser: DE-WIN7\Fwiplayer-Scan Summary-Scan Type: Threat ScanResult: CompletedObjects Scanned: 298073Threats Detected: 12Threats Quarantined: 12Time Elapsed: 2 min, 54 sec-Scan Options-Memory: EnabledStartup: EnabledFilesystem: EnabledArchives: EnabledRootkits: DisabledHeuristics: EnabledPUP: DetectPUM: Detect-Scan Details-Process: 2Backdoor.Agent.DC, C:\USERS\FWIPLAYER\DOCUMENTS\MSDCSC\MSDCSC.EXE, Quarantined, [1570], [218418],1.0.4442Trojan.Agent, C:\USERS\FWIPLAYER\MY DOCUMENTS\MSDCSC\MSDCSC.EXE, Quarantined, [17], [218709],1.0.4442Module: 2Backdoor.Agent.DC, C:\USERS\FWIPLAYER\DOCUMENTS\MSDCSC\MSDCSC.EXE, Quarantined, [1570], [218418],1.0.4442Trojan.Agent, C:\USERS\FWIPLAYER\MY DOCUMENTS\MSDCSC\MSDCSC.EXE, Quarantined, [17], [218709],1.0.4442Registry Key: 1Backdoor.DarkComet.Trace, HKU\S-1-5-21-2165681608-3755637219-621560601-1000\SOFTWARE\DC3_FEXEC, Delete-on-Reboot, [13190], [246706],1.0.4442Registry Value: 1Backdoor.Agent.DC, HKU\S-1-5-21-2165681608-3755637219-621560601-1000\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN|MicroSystem, Delete-on-Reboot, [1570], [218418],1.0.4442Registry Data: 2Backdoor.Agent.DC, HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON|Userinit, Replace-on-Reboot, [1570], [218418],1.0.4442Hijack.UserInit, HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON|USERINIT, Replace-on-Reboot, [1402], [291753],1.0.4442Data Stream: 0(No malicious items detected)Folder: 0(No malicious items detected)File: 4Backdoor.Agent.DC, C:\USERS\FWIPLAYER\DOCUMENTS\MSDCSC\MSDCSC.EXE, Delete-on-Reboot, [1570], [218418],1.0.4442Trojan.Agent, C:\USERS\FWIPLAYER\MY DOCUMENTS\MSDCSC\MSDCSC.EXE, Delete-on-Reboot, [17], [218709],1.0.4442Backdoor.DarkComet, C:\USERS\FWIPLAYER\DESKTOP\2C0F015C0C1E1F8399E9AE975109D3F8.EXE, Delete-on-Reboot, [328], [500877],1.0.4442Backdoor.DarkComet, C:\USERS\FWIPLAYER\DOWNLOADS\2C0F015C0C1E1F8399E9AE975109D3F8, Delete-on-Reboot, [328], [500877],1.0.4442Physical Sector: 0(No malicious items detected)

Source: https://blog.malwarebytes.com/detections/backdoor-darkcomet/