How to protect remote desktop from malware RDStealer

RDStealer is malware that tries to steal credentials and data by infecting an RDP server and monitoring its remote connections.

The process of identifying new and emerging cybersecurity threats never ends - and in June 2023, BitDefender Labs discovered a piece of malware targeting systems using remote desktop connections since 2022.

If you use Remote Desktop Protocol (RDP), it is important to determine if you are a target and if your data has been stolen. Fortunately, there are several methods you can use to prevent infection and remove RDStealer from your PC.

What is RDStealer? How were you targeted?

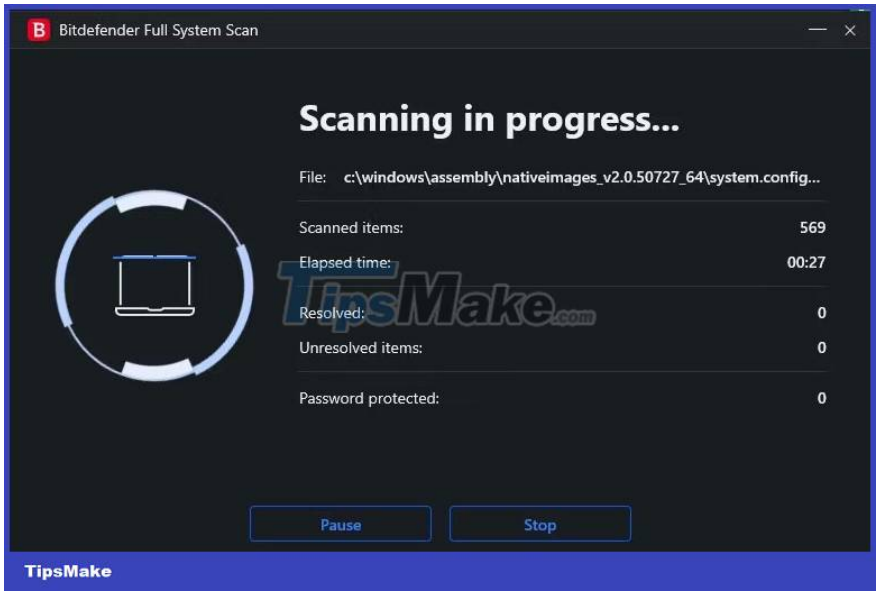
RDStealer is malware that tries to steal credentials and data by infecting an RDP server and monitoring its remote connections. RDStealer deploys alongside Logutil, a backdoor used to infect remote desktops and allows persistent access through client-side RDStealer installation.

If the malware detects that a remote machine has connected to the server and Client Drive Mapping (CDM) is enabled, the malware will scan the contents of the machine and look for files such as the KeePass password database, stored passwords in the browser, and SSH private keys. It also collects keystrokes and clipboard data.

RDStealer can target your system regardless of whether it is server side or client side. When RDStealer infects a network, it creates malicious files in directories like **"%WinDir%System32"** and **"%PROGRAM-FILES%"** which are normally excluded during system-wide malware scans.

According to Bitdefender, the malware spreads through several vectors. In addition to the CDM attack vector, RDStealer infections can originate from infected web ads, malicious email attachments, and Social Engineering campaigns. The team responsible for RDStealer seems particularly sophisticated, so new attack vectors - or improved forms of RDStealer - may emerge in the future.

If you use remote desktop via RDP, your safest bet is to assume that RDStealer has infected your system. Although viruses are too smart to be easily identified manually, you can prevent RDStealer by improving security protocols on your server and client systems and by performing a full system virus scan without unnecessary exclusions.



You're especially vulnerable to RDStealer if you're using a Dell system, as it seems to specifically target Dell-made computers. The malware is intentionally designed to disguise itself in folders like **"Program FilesDellCommandUpdate"** and use command-and-control domains like **"dell-a[.]ntp-update[.]com".**

Protect remote desktop against RDStealer

The most important thing you can do to protect yourself against RDStealer is to be cautious when browsing the web. While there aren't many specifics about how RDStealer spreads beyond RDP connections, care should be taken to avoid almost any infection vector.

Use multi-factor authentication

You can improve the security of RDP connections by implementing best practices like multi-factor authentication (MFA). By requiring a secondary authentication method for each login, you can prevent many types of RDP attacks. Other best practices, like implementing network-level authentication (NLA) and using a VPN, can also make your system unattractive and vulnerable.

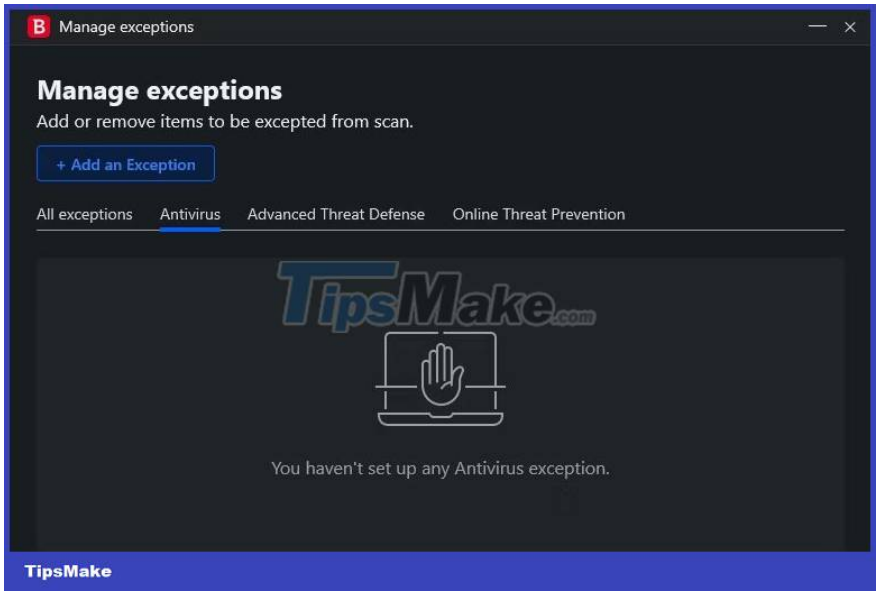
Encryption and data backup

RDStealer effectively steals data - and in addition to plaintext found in the clipboard and obtained from keystrokes, it also looks for files like KeePass Password Databases. While stolen data has no positive side, you can rest assured that any stolen data will be difficult to deal with if you diligently encrypt your files.

File encryption is a relatively simple task with the right guidance. It is also extremely effective in protecting files, as hackers will need to go through a difficult process to decrypt encrypted files. While it's possible to decrypt files, hackers are more likely to turn to easier targets - and as a result, you're completely invulnerable. In addition to encryption, you should also regularly back up your data to avoid losing access later.

Configure your anti-virus software correctly

Configuring your anti-virus software correctly is also important if you want to protect your system. RDStealer takes advantage of the fact that many users will exclude entire directories instead of specifically recommended files by creating malicious files in these directories. If you want your antivirus to find and remove RDStealer, you need to change the exclusions to include only specifically recommended files.



For reference, RDStealer creates malicious files in directories (and their respective subdirectories) including:

1. %WinDir%System32
2. %WinDir%System32wbem
3. %WinDir%securitydatabase
4. %PROGRAM_FILES%f-securepsbdiagnostics
5. %PROGRAM_FILES_x86%dellcommandupdate
6. %PROGRAM_FILES%dellmd storage softwaremd configuration utility

You should adjust your virus scan exclusions according to the guidelines recommended by Microsoft. Excludes only the specified file types and directories and does not exclude parent directories. Verify that your anti-virus software is up to date and complete a full system scan.

Update the latest security news

While the Bitdefender development team has allowed users to protect their systems from RDStealer, it's not the only malware you have to worry about - and there's always the possibility that it will evolve in new and unexpected ways. One of the most important steps you can take to protect your systems is to stay up to date with the latest news on emerging cybersecurity threats.

You finished reading the article "**How to protect remote desktop from malware RDStealer**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.