T-RAT 2.0: Controlling Malware via Telegram

By Karsten Hahn

Published: 2021-04-22 · Archived: 2026-04-05 19:38:49 UTC

T-RAT has 98 commands. Instead of describing every single command within the main article, I categorized them into groups which are explained below. The full command listing is in Appendix B.

1. Menu navigation

These are commands to enter or exit certain modules like the file manager. They help to make controls via smartphone more convenient.

2. File manager

T-RAT can navigate on the file system, show information about the drives and available space, folder contents and modify files and folders. It can also send files to the attacker. Interestingly it mixes in Unix command names. E.g., the file listing is done with **ls**.

3. Stealer

This module allows to obtain passwords, cookies, autofill data from browsers, session or config data of Telegram, Discord, Steam, Nord, Viber, Skype and Filezilla. Most of the data files are either saved besides the T-RAT executable in text files or to a ZIP archive in **%TEMP%/winsys/** before being sent to Telegram.

4. Clipper

The clipper checks the clipboard for coin addresses and replaces them, thus, any digital currency is sent to the attacker's wallet. It supports Qiwi, WMR, WMZ, WME, WMX, Yandex money, Payeer, CC, BTC, BTCG, Ripple, Doge and Tron. The attackers uses the clipper commands to save their addresses for the specified crypto currency and to start or stop execution of the clipper.

5. Monitoring and spying

Enables the attacker to run a keylogger, create screenshots, record audio via the microphone, take pictures via webcam, send clipboard contents.

6. Evasion

T-RAT has various methods to bypass UAC, including Fodhelper, Cmstp, Cleanup, Computerdefaults. It can disable Windows Defender and Smart Screen notifications. It can disable various security settings, e.g.,

Association policies can be changed to set ".exe" as a low-risk file extension, and ZoneIdentifiers can be turned off. It has a check for sandboxes and virtual machines.

7. Disruption

These commands kill processes, block websites via the hosts file, block and redirect programs by setting a debugger via Image File Execution Options (for blocking the debugger is one that doesn't exist), disable the taskbar and the task manager.

8. Remote control

T-RAT provides a **Powershell** or **CMD** terminal via Telegram. Remote control can also be done via **HRDP** or **VNC**.

T-RAT runs the HRDP client named **service\in.exe** which resides in the executable's location. Then it will create a new user account with a randomized password and name and send the credentials to the attacker. It adds the newly created user to the **Remote Desktop Users** group and enables remote access by setting **fDenyTSConnections** to "0".

The VNC server is **service\winserv1.exe** on 32 bit systems and **service\winserv2.exe** on 64 bit systems.
