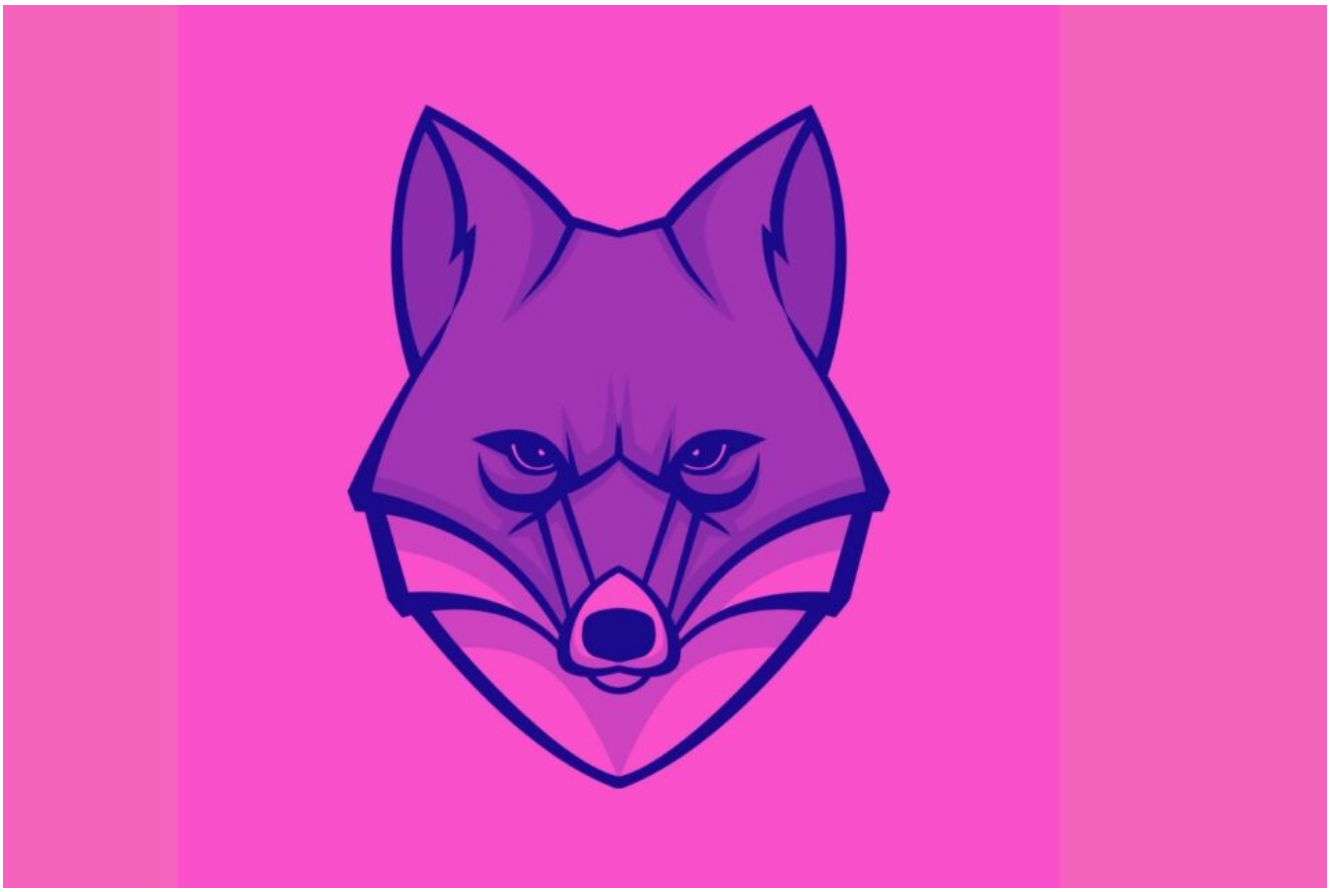
Purple Fox malware is actively distributed via Telegram Installers

John Greenwood Posted On January 4, 2022



Purple Fox malware is distributed via malicious Telegram Desktop Installer, this malware installs further payloads on the affected devices.

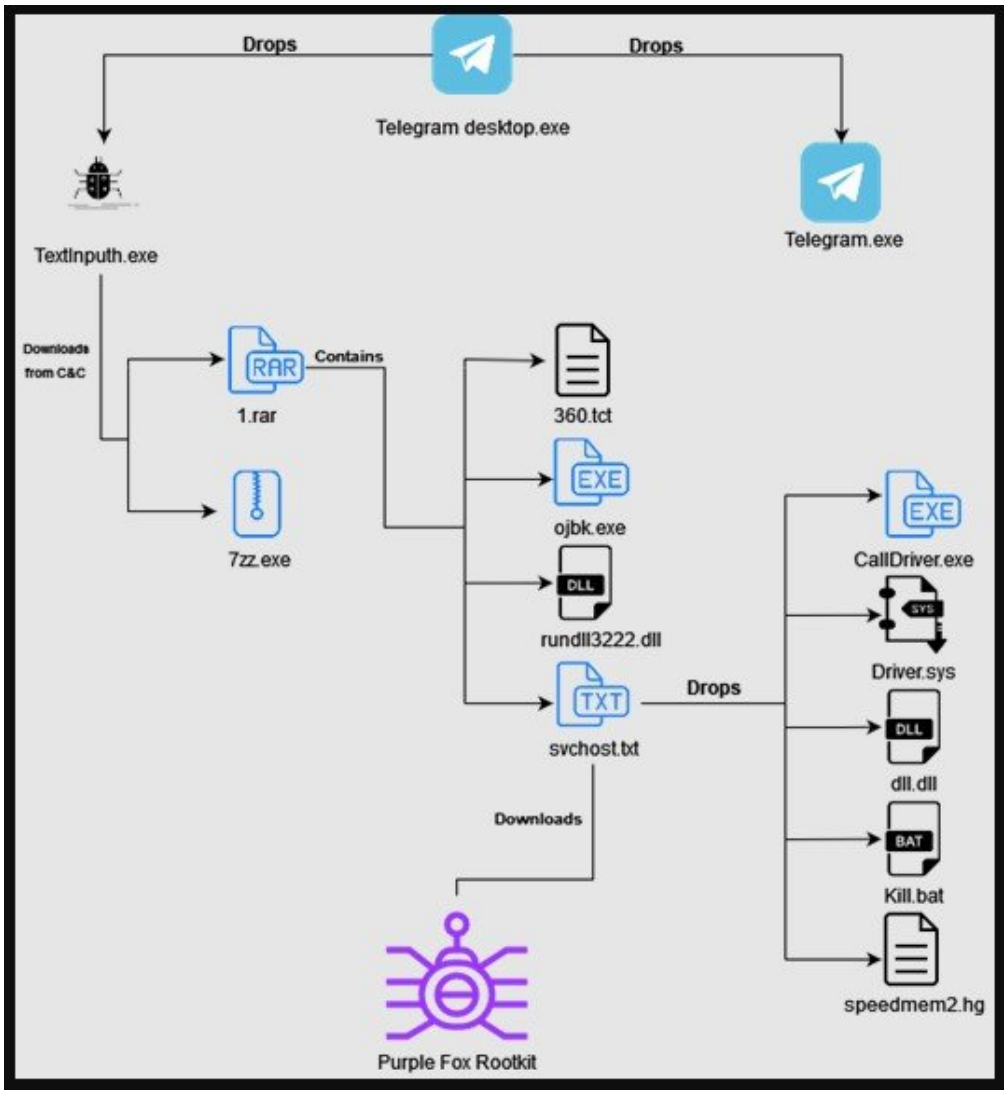
The file “Telegram Desktop.exe” comes with two files, an original installer file and a malicious downloader.The legitimate installer isn’t executed as the AutoIT program runs the TextInputh.exe file.

Understanding the Purple Fox Malware campaign

This TextInputh.exe when executed will create a new folder called “1640618495” under the C:\Users\Public\Videos\ location and then communicate with C2 to download a RAR and 7z utility. The RAR file contains the configuration and payload file, when the 7z program unzips everything to the ProgramData folder.

As per Minerva Labs, TextInputh.exe does the following actions onto the compromised machine,

- Copies 360.tct with “360.dll” name —> rundll3222.exe —-> svchost.txt to the ProgramData folder
- Executes ojbk.exe with the “ojbk.exe -a” command line
- Deletes 1.rar and 7zz.exe and exits the process



Later, a registry key is created and a DLL disables UAC the payload is executed and the following five additional files are dropped into the infected system,

- Calldriver.exe
- Driver.sys
- dll.dll
- kill.bat
- speedmem2.hg

These extra files is used to block the initiation of 360 AV processes and avoid detection of **Purple Fox** on the affected device. Moving further the malware gather system details, scans for security tools running in the device and then send the hard coded C2 address.

Complete capabilities of Purple Fox malware

After this process, **Purple Fox** is downloaded from the C2 in the form of an .msi file that has encrypted shellcode for both 64- and 32- bit systems. Once the Purple Fox is executed, the compromised devices are restarted for the registry settings to work, especially the disabled User Account Control (UAC).

To achieve this, the dll.dll file sets the following three registry keys to 0:

1. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ConsentPromptBehaviorAdmin
2. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
3. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop

Disabling bypassing UAC is vital because it deploys viruses and malware with administrator privileges. In general, UAC prevents the installation of unauthorized apps and the change of system settings, to be active on all Windows devices.

When disabled Purple Fox will perform malicious functions like searching of file, exfiltration, deletion of data, process killing, downloading and running code. and even worming to other Windows devices. Malware similar to Purple Fox are actively being distributed via Youtube Videos, malicious websites, and other forum sites.

Subscribe to our newsletter for daily alerts on cyber events, you can also follow us on Facebook, Linkedin, Instagram, Twitter and Reddit. You can reach out to us via Twitter or Facebook, for any advertising requests.

Author

John Greenwood

He has been working with Cybersec and Infosec market for 12+ years now. Passionate about AI, Cybersecurity, Info security, Blockchain and Machine Learning. When he is not occupied with cybersecurity, he likes to go on bike rides!