In search of the Triangulation: triangle_check utility

By Igor Kuznetsov

Published: 2023-06-02 · Archived: 2026-04-05 16:40:07 UTC

Software

Software

02 Jun 2023

2 minute read

UPD 23.04.2025: MITRE created [a page for Operation Triangulation] as part of its ATT&CK framework.

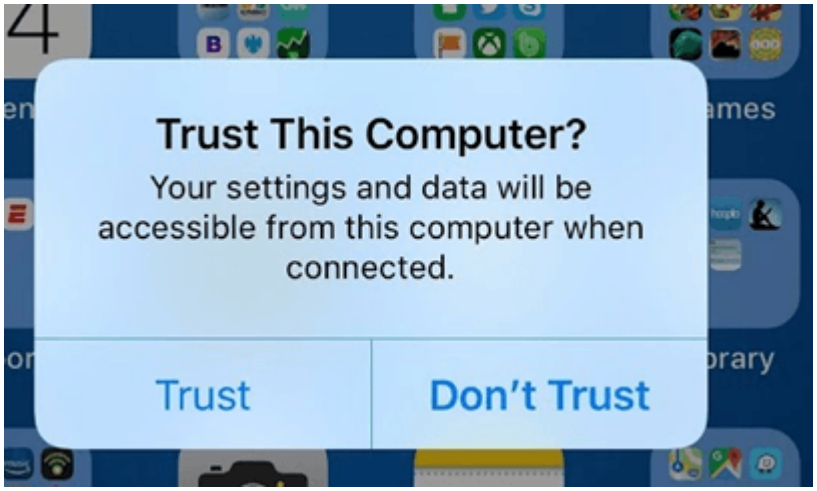
In our [initial blogpost] about “Operation Triangulation”, we published a comprehensive guide on how to manually check iOS device backups for possible indicators of compromise using MVT. This process takes time and requires manual search for several types of indicators. To automate this process, we developed a dedicated utility to scan the backups and run all the checks. For Windows and Linux, this tool can be downloaded as [a binary build], and for MacOS it can be simply installed as [a Python package].

How to back up your device

Windows

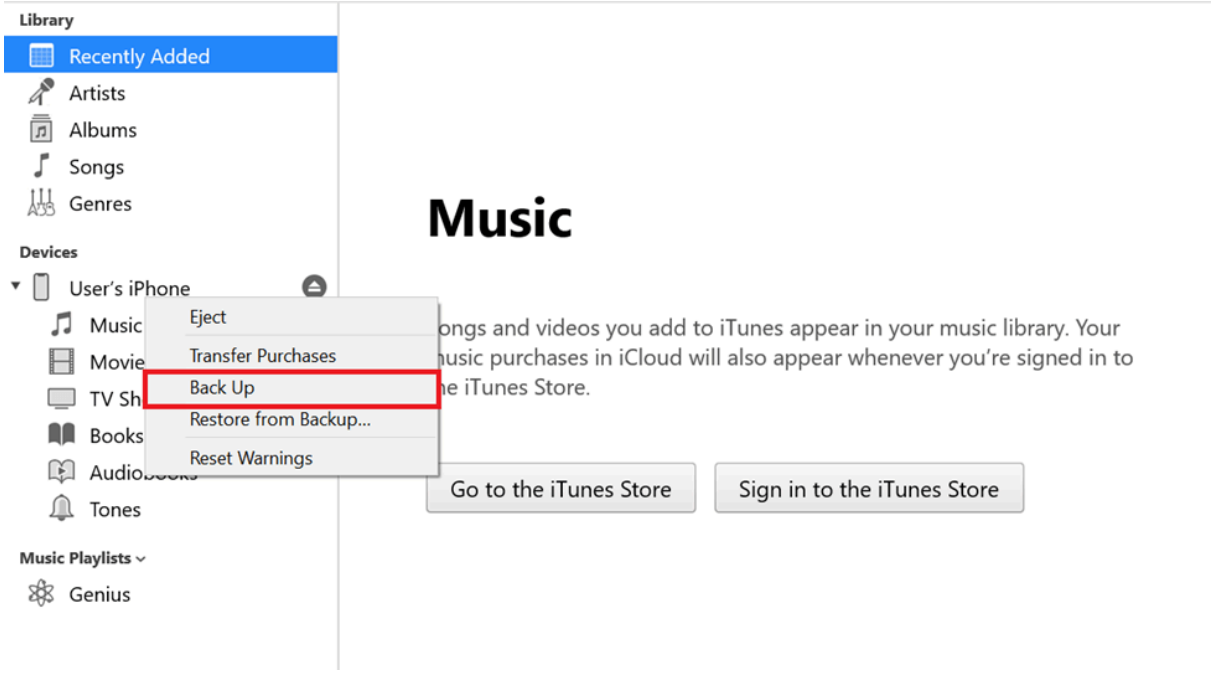
On Windows, the easiest way to do a backup is via iTunes:

1. 1 Connect your device to a computer that has iTunes installed. Unlock your device and, if needed, confirm that you trust your computer.



Window asking to trust the computer

2. 2 Your device should now be displayed in iTunes. Right click on it and press “Back Up”.



3. 3 The created backup will be saved to the *%appdata%\Apple Computer\MobileSync\Backup directory*.

macOS

If your macOS version is lower than Catalina (10.15), you can create a backup using iTunes, using instructions for Windows. Starting from Catalina, backups can be created through Finder:

- Connect your device to the computer and, if needed, confirm that you trust the computer.
- Your device should now be displayed in Finder. Select it and then click “*Create a backup*“.
- The created backup will be saved to the *~/Library/Application Support/MobileSync/Backup/* directory.

Linux

To create a backup on Linux, you will need to install the libimobiledevice library. In order to create backups of devices with the latest versions of iOS installed, you will need to compile this library from source code (you can find the build instructions in the Installation/Getting Started section).
After you install the library and connect your device to the computer, you can create a backup using the `idevicebackup2 backup --full` command.
During the backup process, you may need to enter your device passcode multiple times.

How to use our triangle_check utility

After you do a backup of your device using the instructions above, you will need to install and launch our triangle_check utility.

The triangle_check Python package

No matter what operating system you have, you can install the triangle_check Python package that we have published to the Python Package Index (PyPi). To do that, you need to have internet access as well as have the pip utility installed.
You can install the utility using two methods:

- From PyPI (recommended):
  Run the `python -m pip install triangle_check` command.
- Building from Github:
  Run the following commands:
  ```
  git clone https://github.com/KasperskyLab/triangle_check
  cd triangle_check
  python -m build
  python -m pip install dist/triangle_check-1.0-py3-none-any.whl
  ```

After installing, you can launch the utility with the following command:
`python -m triangle_check *path to the created backup*`.

Binary builds

If you have Windows or Linux, you can also use the binary builds of the triangle_check utility that we have published on GitHub. Follow the instructions below to use it:

Windows

1. 1 Download the triangle_check_win.zip archive from the GitHub releases page and unpack it.
2. 2 Launch the command prompt (cmd.exe) or PowerShell.
3. 3 Change your directory to the one with the unpacked archive (e.g. `cd %userprofile%\Downloads\triangle_check_win`).
4. 4 Launch triangle_check.exe, specifying the path to the backup as an argument (e.g. `triangle_check.exe "%appdata%\Apple Computer\MobileSync\Backup\00008101-000824411441001E-20230530-143718"`).

Linux

1. 1 Download the triangle_check_win.zip archive from the GitHub releases page and unpack it.
2. 2 Launch the terminal.
3. 3 Change your directory to the one with the unpacked archive (e.g. `cd ~/Downloads/triangle_check_linux`).
4. 4 Allow the utility to be executed with the `chmod +x triangle_check` command.
5. 5 Launch the utility, specifying the path to the backup as an argument (e.g. `./triangle_check ~/Desktop/my_backup/00008101-000824411441001E-20230530-143718`).

Interpreting the results

The utility outputs “DETECTED” when it locates specific indicators of compromise, and that would mean that the device was infected.
Also, it may print out “SUSPICION” that would mean that a combination of less specific indicators points to a

likely infection. Finally, if the message displayed is “No traces of compromise were identified“, then the utility did not find any signs of ‘Operation Triangulation’ compromise.

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT’s infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
