What is Malware Fork Bomb? How does it work?

Cybercriminals organize attacks using code snippets. They can try to steal personal information from the computer or damage the entire system.

Cybercriminals don't even need advanced programming and software knowledge to do all that. Did you know that an attacker can completely crash a computer with just one line of code? The name of the method used by threat actors for such attacks is the fork bomb, or rabbit virus.

So what is fork bomb? How do they work? How can you protect yourself?

What is Fork Bomb Virus?

Programming languages ??often produce specific outputs. You write code and when you run it, you will get certain results. But what if these results give program commands that can be run over and over again? In such cases, the program will continue to run indefinitely. The hardware, which is your actual machine, won't be able to run the same thing over and over again; so it will become unusable. In this situation, at the very least, you will have to restart the machine. But even that didn't stop the Fork Bomb.

Fork bomb is a denial of service (DOS) attack, meaning it will use up your RAM so that no legitimate process can take place. That's exactly what a DOS attack does: It denies your service by redirecting resources elsewhere.

This attack can be performed on all operating systems. If you can write code in a simple text file and name the file with an extension that the computer can execute, then your fork bomb is ready. If you want to see the effects for yourself, try it on an isolated environment like a virtual machine. However, it's best not to try.

How does the Script Fork Bomb work?

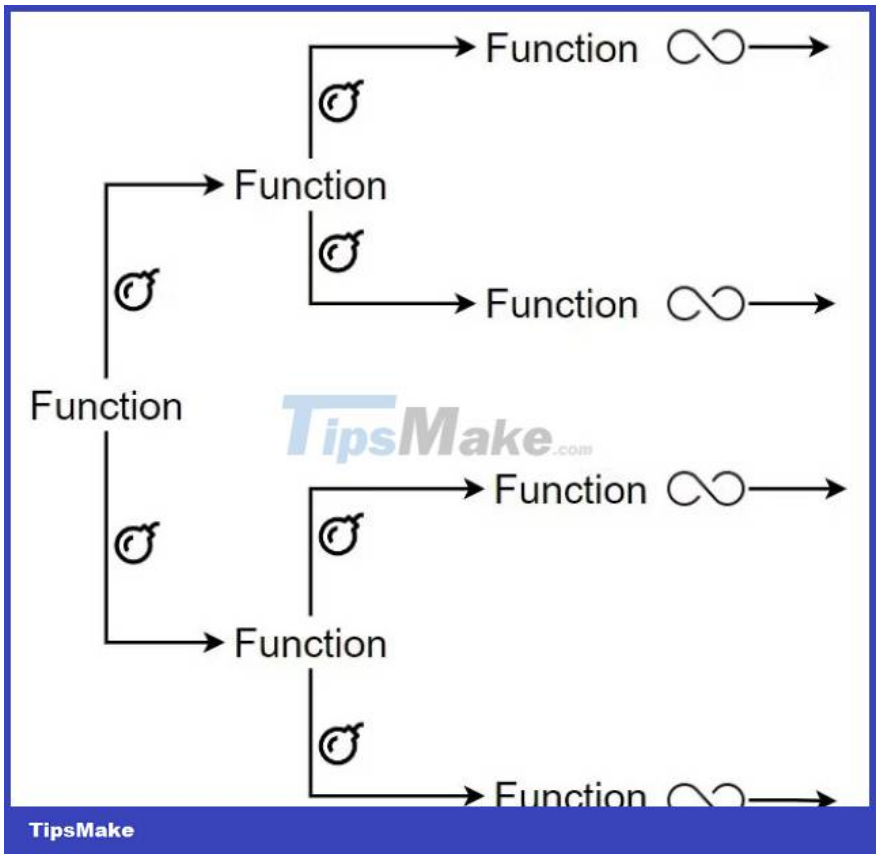
Fork Bomb basically consists of mutual activation functions. Think of it like bacteria starting to reproduce in a container. Bacteria divide and multiply continuously if the necessary conditions and environment are provided. From just one bacteria in a container, tens of thousands of bacteria can form in a few hours. Just like that, the fork bomb itself creates many new fork bombs and after a while, it starts to eat up the computer's CPU. When the CPU can no longer withstand it, the computer will crash.

For the fork bomb to work, the target user must run these files somehow - the BAT file for Windows, the SH file for Linux, both of which can be run with a simple double click. That's why attackers prepare their fork bombs in these formats.

If an attacker targets Windows, they will save the code fork bomb in a text file as a BAT file. When the target user double clicks on this BAT file, the fork bomb starts working. The running program continuously returns

new outputs and reuses them. Since this process will continue forever, after a while, the computer's system requests will no longer be able to handle it. In fact, the computer is so busy with the fork bomb that the user can't even issue a new command to shut it down. The only solution to this is to restart the computer.

If an attacker chooses Linux as the target device, they will use the SH file instead of the BAT file, because Linux cannot open the BAT file. The code fork bomb that an attacker prepares will be different for Windows and Linux; however, the logic of the code sections is exactly the same. When the target user double-clicks the SH file, the same thing happens on Windows: The system requirements will no longer be able to be met at some point and then the attack will succeed.



So if everything goes back to the way it was when you restart the computer, what is the purpose of this attack? The hacker who designed the fork bomb knows that you will reboot your machine. That's why the fork bomb will also restart, i.e. duplicate itself, every time you restart your PC.

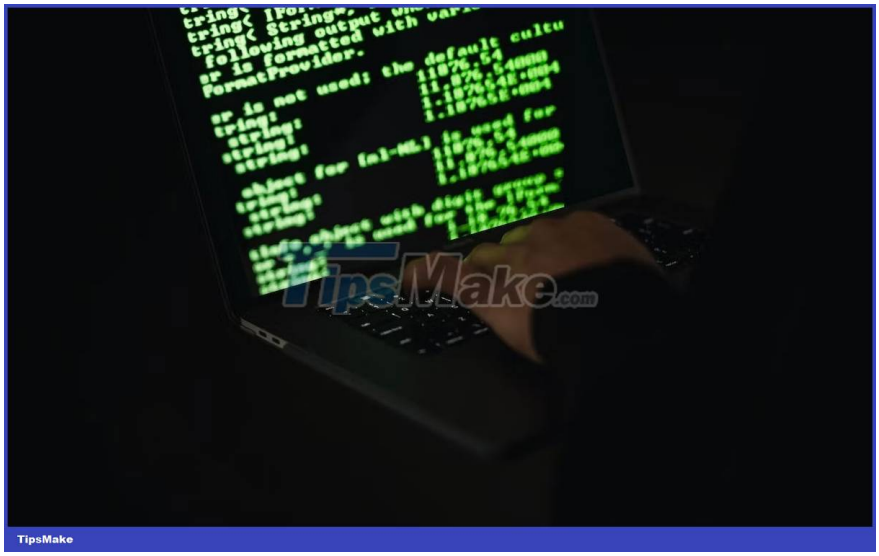
Clicking on these files will render your computer unusable and open a backdoor for malicious attackers. While you are trying to fix your machine, an attacker can steal all your private information.

How to avoid Fork Bomb attacks?

If you rely on anti-virus software to protect your network, you can still be hit with a fork bomb. These code snippets can be small one-line scripts and don't use formats that anti-virus software suites typically suspect, such as .exe files. Antivirus software may not even notice these fork bombs.

The biggest step you should take here is to prevent this malware from getting into your computer. Do not download any files that you are not sure about. No one just randomly sends you SH or BAT files. If you receive such files, whether by email, from a download link on a website or on a social network, do not click on the file.

Antivirus software is not the solution for Fork Bomb



Antivirus software is useful in many ways; No one can denied it. But the fork bomb could be another matter.

The general operating logic of antivirus software is that cybersecurity experts and security researchers discover a new virus or malware. Companies that provide antivirus solutions add this malware to their systems. Now, if you encounter such an attack, the antivirus can warn you because it will recognize this vector. But you are still at risk of unknown malware.

In addition, anti-virus programs consider all program extensions such as EXE, VBS, CMD and MSI, not just BAT or SH files.

For example, if the file you downloaded has the MSI extension, the anti-virus software you are using may suspect the file and warn you about it. But the fork bomb comes in the form of text files and shells. Because the fork bomb is quite lightweight and looks like a text file, some anti-virus software suites may accept such files. In such cases, before opening the file, you should check the contents of the file and, if possible, check the file with a text editor.

You finished reading the article "**What is Malware Fork Bomb? How does it work?**" 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.