Why can’t I trigger a manual blue screen crash by injecting the magic key sequence?

devblogs.microsoft.com/oldnewthing/20240219-00

February 19, 2024

Raymond Chen

A customer was developing an automated test that required the system to suffer a blue screen crash. They configured their test systems to crash when the `ScrollLock` key is pressed twice while holding the `Ctrl` key, and they wrote a simple program that ran as administrator and injected the appropriate keystrokes. But no crash occurred. What did they do wrong?

The key sequence for triggering a manual blue screen crash must be typed on a physical keyboard. Injection doesn’t work.

You may have gotten a clue that the physical keyboard was part of the story since enabling the diagnostic key sequence requires you to apply a different setting depending on what kind of keyboard you are using: There is one setting for PS/2 keyboards, and another for USB keyboards, and yet another for Hyper-V keyboards. It is clear that they keyboard driver is somehow involved.

There is another remark later on the page that talks about limitations of the USB keyboard driver, since it runs at a lower IRQL than the PS/2 driver.

The sequence must be pressed on a physical keyboard because it is the keyboard driver that recognizes the key sequence and triggers the crash screen. Injecting the keys into the window manager is inserting the keypresses at far too high a level in the input stack.

	Input routing	
	↑	
	Input processing	
↗	↑	↖

Keyboard driver	Mouse driver	SendInput
↑	↑	
Hardware keyboard	Hardware mouse	

The best way to trigger an artificial kernel crash is to use NotMyFault, part of the SysInternals family of tools.

Please do not use sneaky tricks like terminating critical processes like `winlogon.exe`. These failures get reported through the Watson service as a `winlogon.exe` crash, which creates confusing among the `winlogon.exe` team as they try to identify the source of a nonexistent bug. If you use NotMyFault, then the system recognizes that the crashes were initialted by NotMyFault, and the Windows team knows that any crashes initiated by that tool were intentional and not an indicator of a system problem that needs to be debugged.