DoublePulsar

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/DoublePulsar#mw-head)[Jump to search](https://en.wikipedia.org/wiki/DoublePulsar#searchInput)

*For the only known double pulsar star system, see*[*PSR J0737-3039*](https://en.wikipedia.org/wiki/PSR_J0737-3039)*.*

|  |  |
| --- | --- |
| **Pulsar Vulnerability** | |
| **Technical name** | * **Double Variant**   + Trojan:Win32/DoublePulsar ([Microsoft](https://en.wikipedia.org/wiki/Microsoft))   + Backdoor.DoublePulsar ([Fortiguard](https://en.wikipedia.org/w/index.php?title=Fortiguard&action=edit&redlink=1)) * **Dark Variant**   + Trojan.Darkpulsar ([Symantec](https://en.wikipedia.org/wiki/NortonLifeLock))[[1]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-1)   + Win32/Equation.DarkPulsar ([ESET](https://en.wikipedia.org/wiki/ESET))[[2]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-2) |
| **Family** | Pulsar (backdoor family) |
| **Author(s)** | [Equation Group](https://en.wikipedia.org/wiki/Equation_Group) |

**DoublePulsar** is a [backdoor](https://en.wikipedia.org/wiki/Backdoor_(computing)) implant tool developed by the U.S. [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency)'s (NSA) [Equation Group](https://en.wikipedia.org/wiki/Equation_Group) that was leaked by [The Shadow Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers) in early 2017.[[3]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-scmagazine-3) The tool infected more than 200,000 [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) [computers](https://en.wikipedia.org/wiki/Computers_in_the_classroom) in only a few weeks,[[4]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-4)[[5]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-usbguy-5)[[3]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-scmagazine-3)[[6]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-6)[[7]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-7) and was used alongside [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue) in the May 2017 [WannaCry ransomware attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack).[[8]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-8)[[9]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-9)[[10]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-10) A variant of DoublePulsar was first seen in the wild in March 2016, as discovered by Symantec. [[11]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-11)

Sean Dillon, senior analyst of security company [RiskSense Inc.](https://en.wikipedia.org/w/index.php?title=RiskSense_Inc.&action=edit&redlink=1), first dissected and inspected DoublePulsar.[[12]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-techanalysis-12)[[13]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-13) He said that the NSA exploits are "10 times worse" than the [Heartbleed](https://en.wikipedia.org/wiki/Heartbleed) security bug, and use DoublePulsar as the primary [payload](https://en.wikipedia.org/wiki/Payload_(computing)). DoublePulsar runs in [kernel mode](https://en.wikipedia.org/wiki/Kernel_mode), which grants cybercriminals a high level of control over the computer system.[[5]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-usbguy-5) Once installed, it uses three commands: [ping](https://en.wikipedia.org/wiki/Ping_(networking_utility)), [kill](https://en.wikipedia.org/wiki/Exit_(system_call)), and [exec](https://en.wikipedia.org/wiki/Exec_(system_call)), the latter of which can be used to load [malware](https://en.wikipedia.org/wiki/Malware) onto the system.[[12]](https://en.wikipedia.org/wiki/DoublePulsar#cite_note-techanalysis-12)