

DoublePulsar

By Contributors to Wikimedia projects

Published: 2017-05-15 · Archived: 2026-04-05 16:50:39 UTC

From Wikipedia, the free encyclopedia

For the only known double pulsar star system, see [PSR J0737-3039](#).

DoublePulsar	
Malware details	
Technical name	<ul style="list-style-type: none">• Double Variant<ul style="list-style-type: none">◦ Trojan:Win32/DoublePulsar (Microsoft)◦ Backdoor.DoublePulsar (Fortiguard)• Dark Variant<ul style="list-style-type: none">◦ Trojan.Darkpulsar (Symantec)^[1]◦ Win32/Equation.DarkPulsar (ESET)^[2]
Family	Pulsar (backdoor family)
Author	Equation Group

```
~/D/445 > wc -l p445_4_22_17.uniq
5190506 p445_4_22_17.uniq
~/D/445 > wc -l 445_detected
96586 445_detected
~/D/445 > head -30 445_detected
[+] [000 00 03.230] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 09.121] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 09.43] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 06.35] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 06.36] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 06.37] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 42.168] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 35.18] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 35.3] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 35.13] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 35.7] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 35.4] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 05.221] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 85.235] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 85.236] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 85.237] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 53.58] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 06.98] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 04.188] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 46.4] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 65.187] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 72.227] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 07.53] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 07.54] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 04.18] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 4.84] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 27.17] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 27.42] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 59.114] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
[+] [000 00 27.6] DOUBLEPULSAR SMB IMPLANT DETECTED!!!
~/D/445 >
```

DoublePulsar is a [backdoor](#) implant tool developed by the U.S. [National Security Agency](#)'s (NSA) [Equation Group](#) that was leaked by [The Shadow Brokers](#) in early 2017.^{[3][[][citation needed](#)]} The tool infected more than

200,000 [Microsoft Windows computers](#) in only a few weeks,^{[4][5][3][6][7]} and was used alongside [EternalBlue](#) in the May 2017 [WannaCry ransomware attack](#).^{[8][9][10]} A variant of DoublePulsar was first seen in the wild in March 2016, as discovered by Symantec.^[11]

Sean Dillon, senior analyst of security company [RiskSense Inc.](#), first dissected and inspected DoublePulsar.^{[12][13]} He said that the NSA exploits are "10 times worse" than the [Heartbleed](#) security bug, and use DoublePulsar as the primary [payload](#). DoublePulsar runs in [kernel mode](#), which grants cybercriminals a high level of control over the computer system.^[5] Once installed, it uses three commands: [ping](#), [kill](#), and [exec](#), the latter of which can be used to load [malware](#) onto the system.^[12]

- ¹ ↑ "[Trojan.Darkpulsar](#)". *Symantec*. Archived from [the original](#) on 3 October 2019.
- ² ↑ "[Win32/Equation.DarkPulsar.A | ESET Virusradar](#)". *www.virusradar.com*.
- ³ ↑ Jump up to: ^a ^b "[DoublePulsar malware spreading rapidly in the wild following Shadow Brokers dump](#)". 25 April 2017.
- ⁴ ↑ Sterling, Bruce. "[Double Pulsar NSA leaked hacks in the wild](#)". *Wired*.
- ⁵ ↑ Jump up to: ^a ^b "[Seriously, Beware the 'Shadow Brokers'](#)". *Bloomberg*. 4 May 2017 – via [www.bloomberg.com](#).
- ⁶ ↑ "[Wana Decrypt0r Ransomware Using NSA Exploit Leaked by Shadow Brokers Is on a Rampage](#)".
- ⁷ ↑ "[>10,000 Windows computers may be infected by advanced NSA backdoor](#)". 21 April 2017.
- ⁸ ↑ Cameron, Dell (13 May 2017). "[Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It](#)".
- ⁹ ↑ Fox-Brewster, Thomas. "[How One Simple Trick Just Put Out That Huge Ransomware Fire](#)". *Forbes*.
- ¹⁰ ↑ "[Player 3 Has Entered the Game: Say Hello to 'WannaCry'](#)". *blog.talosintelligence.com*. 12 May 2017. Retrieved 2017-05-15.
- ¹¹ ↑ "[Stolen NSA hacking tools were used in the wild 14 months before Shadow Brokers leak](#)". *arstechnica.com*. 7 May 2019. Retrieved 2019-05-07.
- ¹² ↑ Jump up to: ^a ^b "[DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis](#)". *zerosum0x0.blogspot.com*. 21 April 2017. Retrieved 2017-05-16.
- ¹³ ↑ "[NSA's DoublePulsar Kernel Exploit In Use Internet-Wide](#)". *threatpost.com*. 24 April 2017. Retrieved 2017-05-16.

Source: <https://en.wikipedia.org/wiki/DoublePulsar>