DoublePulsar

By Contributors to Wikimedia projects

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

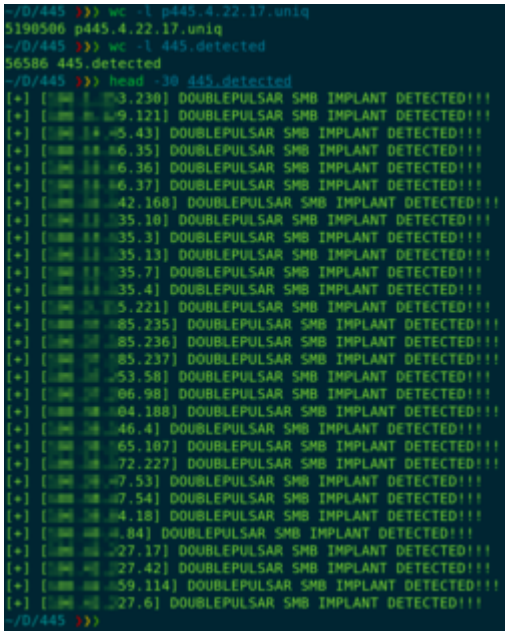
From Wikipedia, the free encyclopedia

For the only known double pulsar star system, see PSR J0737-3039.

DoublePulsar	
Malware details	

Technical name	• **Double Variant**
	  ◦ Trojan:Win32/DoublePulsar (Microsoft)
	  ◦ Backdoor.DoublePulsar (Fortiguard)
	• **Dark Variant**
	  ◦ Trojan.Darkpulsar (Symantec)[1]
	  ◦ Win32/Equation.DarkPulsar (ESET)[2]

Family	Pulsar (backdoor family)
Author	Equation Group



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.*
