Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:43:19 UTC

Tool: DoublePulsar

Names	DoublePulsar
Category	Malware
Type	Loader
Description	(Trend Micro) DoublePulsar is a memory-based kernel payload that allows attackers to inject arbitrary Dynamic-link Library (DLL) files to the system processes and execute shellcode payloads, ultimately providing attackers unprecedented access to infected x86 and 64-bit systems. Trend Micro's continuous analysis of the dump suggests that EternalBlue is one of the exploits that also executes DoublePulsar as payload. EternalBlue is part of the Fuzzbunch framework (also found in the dump) responsible for executing the exploits.
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malware-using-exploits-from-shadow-brokers-in-the-wild> <https://countercept.com/our-thinking/doublepulsar-usermode-analysis-generic-reflective-dll-loader/> <https://countercept.com/our-thinking/analyzing-the-doublepulsar-kernel-dll-injection-technique/> <https://github.com/countercept/doublepulsar-c2-traffic-decryptor> <https://labs.nettitude.com/blog/a-quick-analysis-of-the-latest-shadow-brokers-dump/> <https://en.wikipedia.org/wiki/DoublePulsar>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.doublepulsar>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DoublePulsar>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool DoublePulsar

Changed	Name	Country	Observed

APT groups

	APT 3, Gothic Panda, Buckeye		2007-Nov 2017	
	Calypso		2016-Aug 2021	
	Equation Group		2001-Aug 2016	
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	
	Turla, Waterbug, Venomous Bear		1996-2024	
	Wicked Spider, APT 22		2018	

6 groups listed (6 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=15f91367-9891-423d-9c11-060172f7a7f6