Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:38:38 UTC

Tool: EternalBlue

Names	EternalBlue
Category	Exploits
Type	0-day
Description	(Check Point) The EternalBlue exploitation tool was leaked by "The Shadow Brokers" group on April 14, 2017, in their fifth leak, "Lost in Translation." The leak included many exploitation tools like EternalBlue that are based on multiple vulnerabilities in the Windows implementation of SMB protocol. EternalBlue works on all Windows versions prior to Windows 8. These versions contain an interprocess communication share (IPC$) that allows a null session. This means that the connection is established via anonymous login and null session is allowed by default. Null session allows the client to send different commands to the server.
Information	<https://research.checkpoint.com/2017/eternalblue-everything-know/> <https://cybernews.com/security/eternalblue-vulnerability-exploit-explained/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:EternalBlue>

Last change to this tool card: 06 September 2023

Download this tool card in JSON format

All groups using tool EternalBlue

Changed	Name	Country	Observed	
APT groups				
	APT 3, Gothic Panda, Buckeye		2007-Nov 2017	
	Calypso		2016-Aug 2021	

	Chafer, APT 39		2014-Sep 2020	
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	
	Turla, Waterbug, Venomous Bear		1996-2024	
	Wicked Spider, APT 22		2018	

7 groups listed (7 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=cb1f1730-b938-44da-99ef-a15d7b16fee2