Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:51:47 UTC

Tool: PORTHOLE

Names	PORTHOLE
Category	Malware
Type	Reconnaissance
Description	(Mandiant) FIN13 used PORTHOLE, a Java-based port scanner, to conduct network research. PORTHOLE may attempt multiple socket connections to many IPs and ports and, as it is multi-threaded, can execute this operation rapidly with potentially multiple overlapping connections. The malware accepts as its first argument either an IP address with wildcards in the address, or a filename. The second argument is the starting port range to scan for each IP, and the third is the ending port range.
Information	<https://www.mandiant.com/resources/fin13-cybercriminal-mexico>

Last change to this tool card: 26 December 2021

Download this tool card in JSON format

All groups using tool PORTHOLE

Changed	Name	Country	Observed	
APT groups				
	FIN13	[Unknown]	2016	

1 group listed (1 APT, 0 other, 0 unknown)