Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:45:50 UTC

Tool: CLOSEWATCH

Names	CLOSEWATCH
Category	Malware
Type	Backdoor
Description	(Mandiant) CLOSEWATCH is a JSP web shell that communicates with a listener on localhost over a specified port, writes arbitrary files to the victim operating system, executes arbitrary commands on the victim host, disables proxying and issues customizable HTTP GET requests to a range of remote hosts. If the proper HTTP URL parameters are specified, CLOSEWATCH can create a socket connection to localhost on port 16998 where it can send and receive data using HTTP-like communications using chunked transfer-encoding. If the range parameter is specified, CLOSEWATCH can scan a range of IPs and ports using custom parameters. This malware was observed at one of the earliest FIN13 investigations. Although a sample has recently appeared on a public repository, this malware hasn't been observed during more recent investigations. While more than just a recon tool, CLOSEWATCH's range parameter provides FIN13 with another scanning capability.
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 CLOSEWATCH

Changed	Name	Country	Observed	
APT groups				
	FIN13	[Unknown]	2016	

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