Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:21:10 UTC

Tool: SodomMain

Names	SodomMain SodomMain RAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(Proofpoint) The SodomMain module is LookBack malware's remote access Trojan module that can send and receive numerous commands indicative of its function as a RAT. The malware is delivered within the encoded data that is received by the SodomNormal module as part of its initial beacon response. It then runs within the SodomNormal module and uses its "send_data" function for C&C communications. The data is ultimately relayed to the GUP Proxy Tool and the C&C IP. Noteworthy malware commands include: • Get process listing • Kill process • Executes cmd[.] exe command • Gets drive type • Find files • Read files • Delete files • Write to files • Execute files • Enumerate services • Starts services • Delete services • Takes a screenshot of desktop • Move/Click Mouse and take a screenshot • Exit • Removes self (libcurl[.] dll) • Shutdown • Reboot

Information	<https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool SodomMain

Changed	Name	Country	Observed	
APT groups				
	LookBack, TA410	[Unknown]	2019-Feb 2022	

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