Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:58:05 UTC

Tool: SodomNormal

Names	SodomNormal
Category	Malware
Type	Exfiltration, Tunneling
Description	(Proofpoint) The SodomNormal Communications module runs within the libcurl.dll loader as a loaded DLL. Its primary function is to communicate data gathered by the SodomMain remote access Trojan module with the GUP Proxy Tool. It attempts to acquire an existing configuration from the file sodom.ini. However, it appears the configuration is dropped in the file sodom.txt instead. If that configuration is not available, it utilizes a hardcoded configuration in the binary. The tool uses a custom binary protocol over sockets for its command and control communication with the GUP Proxy Tool and all transferred data is encrypted using a modified version of RC4 encryption. It has limited functionality which includes an initial beacon, an initial beacon response that includes encoded data containing the SodomMain RAT, and a command poll which passes header and decrypted data in an exported function enabling the SodomMain RAT to run.
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 SodomNormal

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

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