Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:21:56 UTC

Tool: SystemBC

Names	SystemBC Coroxy DroxiDat
Category	Malware
Type	Backdoor, Tunneling
Description	(Sophos) First seen in 2019, SystemBC is a proxy and remote administrative tool, named by researchers after the string in the URI its control panel used. It acts both as a network proxy for concealed communications and as a remote administration tool (RAT)—capable of executing Windows commands, and delivering and executing scripts, malicious executables and dynamic link libraries (DLLs). After being dropped by other malware, it provides attackers with a persistent backdoor. While SystemBC has been around for over a year, we've seen both its use and its features continue to evolve. The most recent samples of SystemBC carry code that, instead of acting essentially as a virtual private network via a SOCKS5 proxy, uses the Tor anonymizing network to encrypt and conceal the destination of command and control traffic.
Information	<https://news.sophos.com/en-us/2020/12/16/systembc/> <https://www.proofpoint.com/us/threat-insight/post/systembc-christmas-july-socks5-malware-and-exploit-kits> <http://www.intel471.com/blog/cobalt-strike-cybercriminals-trickbot-qbot-hancitor> <https://www.kroll.com/en/insights/publications/cyber/inside-the-systembc-malware-server>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.systembc>

Last change to this tool card: 06 March 2024

Download this tool card in JSON format

All groups using tool SystemBC

Changed	Name	Country	Observed

APT groups

	Sprite Spider, Gold Dupont	[Unknown]	2015-Nov 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=dd23b5ad-bb56-45fb-9376-dc12ba4147bb