Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:35:36 UTC

Tool: SparrowDoor

Names	SparrowDoor FamousSparrow
Category	Malware
Type	Backdoor
Description	(ESET) The connections could be either through a proxy or not, and they connect to the C&C server over port 443 (HTTPS). So, the communication should be encrypted using TLS. During the first attempt to contact the C&C server, SparrowDoor checks whether a connection can be established without using a proxy, and if it can't, then the data is sent through a proxy. All outgoing data is encrypted using the XOR key hH7@83#mi and all incoming data is decrypted using the XOR key h*^4hFa. The data has a structure that starts with a Command ID, followed by the length of the ensuing encrypted data, followed by the encrypted data.
Information	<https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sparrow_door>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool SparrowDoor

Changed	Name	Country	Observed	
APT groups				
	Salt Typhoon, GhostEmperor		2020-Feb 2025	

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