Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:32:54 UTC

Tool: QueenOfHearts

Names	QueenOfHearts
Category	Malware
Type	Backdoor, Info stealer
Description	(Kaspersky) While it does not contain the anti-analysis countermeasures of its cousin, the rest of its features and overall design decisions map to KingOfHearts almost one to one. QueenOfHearts seems to have appeared somewhere in 2017. It is the family designated as PowerPool by our esteemed colleagues from ESET. QueenOfHearts also interacts with its C2 server over HTTP. It sends simple GET requests containing a backdoor identifier and optional victim machine information, then reads orders located in the cookie header of the reply. Orders come in the form of two-letter codes (e.g.: “xe” to list drives) which tend to vary between samples. As of today, this family is still in active development, and we have observed code refactoring as well as incremental upgrades over 2020. For instance, earlier backdoor responses were sent as base64-encoded payloads in POST requests. They are now compressed beforehand, and additionally supplied through the cookie header.
Information	<https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/>

Last change to this tool card: 19 October 2020

Download this tool card in JSON format

All groups using tool QueenOfHearts

Changed	Name	Country	Observed	
APT groups				
	IAmTheKing		2018	

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