

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:45:09 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool KingOfHearts

## Tool: KingOfHearts

Names	KingOfHearts
Category	<a href="#">Malware</a>
Type	<a href="#">Reconnaissance</a> , <a href="#">Backdoor</a> , <a href="#">Info stealer</a>
Description	<p>(<a href="#">Kaspersky</a>) In terms of capabilities, KingOfHearts offers nothing more than the basic features you would expect from a backdoor:</p> <ul style="list-style-type: none"> <li>• Arbitrary command execution</li> <li>• File system manipulation: listing drives and files, deleting, uploading and downloading data, etc.</li> <li>• Listing of running processes with the option to terminate any of them</li> <li>• Capturing screenshots using a custom standalone utility, described below</li> </ul> <p>Rather than developing sophisticated features, the malware developers instead opted to include anti-debugging and virtualization detection routines. Communications with the C2 server take place over HTTP(S), implemented with the wsdlpull open source library. The backdoor looks for new orders every second by sending a heartbeat to the C2 (the “HEART” command, hence the name).</p>
Information	< <a href="https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/">https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/</a> >

Last change to this tool card: 19 October 2020

Download this tool card in [JSON](#) format

## All groups using tool KingOfHearts

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">IAmTheKing</a>		2018

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

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=c8d96d97-8458-4183-b778-4123781fdc06>