

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:26:01 UTC

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

## Tool: SilverHawk

Names	SilverHawk
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a> , <a href="#">Info stealer</a> , <a href="#">Exfiltration</a>
Description	<p>(<a href="#">Lookout</a>) App Capabilities:</p> <ul style="list-style-type: none"><li>• Record Audio<ul style="list-style-type: none"><li>o Stream environment audio over raw socket when instructed</li></ul></li><li>• Take photos with device camera</li><li>• Survival counter - failed server connections and it stops</li><li>• Retrieve files from external storage<ul style="list-style-type: none"><li>o Top directory</li><li>o Downloads, Pictures, DCIM directories</li><li>o WhatsApp, Telegram, Viber, ShareIt content</li><li>o Files sent over Bluetooth</li></ul></li><li>• File utility to copy, move, rename, and delete files</li><li>• Download attacker specified files</li><li>• Enumerate installed apps incl. date &amp; time installed</li><li>• Attempt to execute attacker specified commands or binary as root</li><li>• Retrieve contacts and related data:<ul style="list-style-type: none"><li>o Call logs</li><li>o Contacts</li><li>o Text Messages</li></ul></li><li>• Location, direction, and acceleration of the device</li><li>• Remotely updateable C2 IP and port</li><li>• Hide Icon</li><li>• Device information<ul style="list-style-type: none"><li>o Retrieve battery levels, WiFi and GPS status, storage and cellular carrier info</li></ul></li></ul>
Information	< <a href="https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-DelRosso-Under-the-SEA.pdf">https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-DelRosso-Under-the-SEA.pdf</a> >

Last change to this tool card: 20 April 2020

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

## All groups using tool SilverHawk

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Syrian Electronic Army (SEA), Deadeye Jackal</a>		2011-Aug 2021 

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

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=ec12d7cd-5480-4511-a333-2b0c4c26c65e>