

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:52:25 UTC

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


## Tool: KeyBoy

Names	KeyBoy TSSL
Category	<a href="#">Malware</a>
Type	<a href="#">Reconnaissance</a> , <a href="#">Backdoor</a> , <a href="#">Info stealer</a> , <a href="#">Exfiltration</a>
Description	<p>(<a href="#">PWC</a>) The malware leveraged by KeyBoy has a plethora of functionality, including, but not limited to:</p> <ul style="list-style-type: none"> <li>• Screen grabbing/taking screenshots;</li> <li>• Determine public or WAN IP address (using a public IP service), likely for determining a suited target;</li> <li>• Gather extended system information, such as information about the operating system, disks, memory and so on;</li> <li>• A ‘file browser’ or explorer;</li> <li>• Shutdown and reboot commands (in addition to the point below);</li> <li>• Launching interactive shells for communicating with the victim machine;</li> <li>• Download and upload functionality; and</li> <li>• Usage of custom SSL libraries for masquerading C2 traffic.</li> </ul>
Information	<p>&lt;<a href="https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html">https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html</a>&gt;</p> <p>&lt;<a href="https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/">https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/</a>&gt;</p> <p>&lt;<a href="https://citizenlab.ca/2016/11/parliament-keyboy/">https://citizenlab.ca/2016/11/parliament-keyboy/</a>&gt;</p> <p>&lt;<a href="https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/">https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/</a>&gt;</p>
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0387/">https://attack.mitre.org/software/S0387/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.keyboy">https://malpedia.caad.fkie.fraunhofer.de/details/win.keyboy</a> >
AlienVault OTX	< <a href="https://otx.alienvault.com/browse/pulses?q=tag:keyboy">https://otx.alienvault.com/browse/pulses?q=tag:keyboy</a> >

Last change to this tool card: 14 May 2020

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

### All groups using tool KeyBoy

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Tropic Trooper</a> , <a href="#">Pirate Panda</a> , <a href="#">APT 23</a> , <a href="#">KeyBoy</a>		2011-Jun 2023

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=dbec73b9-60b1-42a5-a4b3-ab5bef525f2b>