

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:37:18 UTC

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

## Tool: SideWalk

Names	SideWalk ScrambleCross
Category	<a href="#">Malware</a>
Type	<a href="#">Reconnaissance</a> , <a href="#">Backdoor</a>
Description	<a href="#">(ESET)</a> This backdoor shares multiple similarities with another backdoor used by the group: <a href="#">CrossWalk</a> .  SideWalk is a modular backdoor that can dynamically load additional modules sent from its C&C server, makes use of Google Docs as a dead drop resolver, and uses Cloudflare workers as a C&C server. It can also properly handle communication behind a proxy.
Information	< <a href="https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/">https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/</a> > < <a href="https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf">https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf</a> > < <a href="https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware">https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewalk">https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewalk</a> >

Last change to this tool card: 28 December 2021

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

### All groups using tool SideWalk

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">APT 41</a>		2012-Jul 2025	

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

---

Source: <https://apt.eta.doe.gov/cgi-bin/listgroups.cgi?u=7c20f5f1-cf05-4b00-b9d4-f30dae173daa>