Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:50:19 UTC

Tool: ZXShell

Names	ZXShell Sensocode
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Exfiltration, Tunneling, DDoS
Description	(FireEye) ZXSHELL is a backdoor that can be downloaded from the internet, particularly Chinese hacker websites. The backdoor can launch port scans, run a keylogger, capture screenshots, set up an HTTP or SOCKS proxy, launch a reverse command shell, cause SYN floods, and transfer/delete/run files. The publicly available version of the tool provides a graphical user interface that malicious actors can use to interact with victim backdoors. Simplified Chinese is the language used for the bundled ZXSHELL documentation.
Information	<https://paper.bobylive.com/Security/APT_Report/APT-41.pdf> <https://github.com/smb01/zxshell> <https://blogs.cisco.com/security/talos/opening-zxshell>
MITRE ATT&CK	<https://attack.mitre.org/software/S0412/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.zxshell>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:zxshell>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool ZXShell

Changed	Name	Country	Observed
APT groups			

	APT 41		2012-Jul 2025	
	Axiom, Group 72		2008-2008/2014	
	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	
	PassCV		2016	

5 groups listed (5 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b63bf358-4d19-4729-b6bb-dfd6588f44e0