

2.0 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:17:16 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Skip-2.0

Tool: Skip-2.0

Names	Skip-2.0
Category	Malware
Type	Backdoor , Exfiltration
Description	(ESET) This backdoor targets MSSQL Server 11 and 12, allowing the attacker to connect stealthily to any MSSQL account by using a magic password – while automatically hiding these connections from the logs. Such a backdoor could allow an attacker to stealthily copy, modify or delete database content. This could be used, for example, to manipulate in-game currencies for financial gain. In-game currency database manipulations by Winnti operators have already been reported.
Information	< https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.skip20 >

Last change to this tool card: 24 April 2021

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

All groups using tool Skip-2.0

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=39b1fa4d-de40-4fb5-86e5-f50cd9be3b7d>