

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:55:57 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool sqllauncher.dll

Tool: sqllauncher.dll

Names	sqllauncher.dll
Category	Malware
Type	Backdoor
Description	<p>(Avast) Both DLLs, sqllauncher.dll and logon.dll, are primarily used as backdoors. These are installed as services by the aforementioned batch file. They both create a log file under the path: %COMMON_DOCUMENT%\WZ9JuN00.tmp aggregating errors during the backdoor's runtime. Each entry contains an error code, an error message, and a timestamp formatted as “[yyyy-mm-dd hh-mm-ss] %error code% %message%”.</p> <p>If the infected device can't connect to the C&C server, the malware attempts to determine whether the traffic is routed through a proxy. This information may be retrieved either from %WINDOWS%\debug\netlogon.cfg or from the TCP table. After successfully connecting to the C&C server, a secure communication channel (Schannel) is established and telemetry (OS version, username) is sent to the C&C server.</p>
Information	< https://decoded.avast.io/luigicamasta/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/ >

Last change to this tool card: 18 May 2020

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

All groups using tool sqllauncher.dll

Changed	Name	Country	Observed
APT groups			
	Mikroceen		2017-Mar 2021

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=5721d5f1-1bc1-446b-87d8-28d0b619bcc7>