

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:01:26 UTC

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

↪ Tool: Excalibur

Names	Excalibur Sabresac Saber
Category	Malware
Type	Backdoor
Description	<p>(Cylance) Saber is a custom RAT that periodically queries a web-based C2 server for commands. The only active instances SPEAR was able to identify were hosted on the Chinese code development site 'csdn(dot)net'. Kitkiot variants are commonly installed alongside other types of malware and often included additional functionality, including:</p> <ul style="list-style-type: none"> • Denial of Service (DoS) and Distributed Denial of Service (DDoS) capabilities • The ability to hijack and steal in-game account information and items from multiple online gaming platforms • In some rare cases these were used for click-through advertising fraud.
Information	< https://threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.excalibur >

Last change to this tool card: 23 April 2020

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

All groups using tool Excalibur

Changed	Name	Country	Observed
APT groups			
	PassCV		2016

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

Source: <https://apt.eta.da.or.th/cgi-bin/listgroups.cgi?u=7988e6c1-d35e-4a7e-a1b5-5a24c4a4f6ea>