

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:25:43 UTC

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

Tool: Fobber

Names	Fobber
Category	Malware
Type	Banking trojan , Backdoor , Credential stealer
Description	(GovCERT.ch) In the original sample, there was no sign of Man-in-the-Browser (MitB) aiming to steal banking credentials but, since the malware has the capability to update itself, this possibility can be later added by the attackers. On our analysis, apart from the update feature, we only found the form-grabbing / cookie-stealing malicious feature.
Information	<p><https://www.govcert.admin.ch/downloads/whitepapers/govcertch_fobber_analysis.pdf></p> <p><https://www.govcert.ch/blog/analysing-a-new-ebanking-trojan-called-fobber/></p> <p><https://blog.malwarebytes.com/threat-analysis/2015/06/elusive-hanjuan-ek-caught-in-new-malvertising-campaign/></p> <p><http://blog.wizche.ch/fobber/malware/analysis/2015/08/10/fobber-encryption.html></p> <p><http://byte-atlas.blogspot.ch/2015/08/knowledge-fragment-unwrapping-fobber.html></p> <p><https://searchfinancialsecurity.techtarget.com/news/4500249201/Fobber-Drive-by-financial-malware-returns-with-new-tricks></p>
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.fobber >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:Fobber >

Last change to this tool card: 24 May 2020

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

All groups using tool Fobber

Changed	Name	Country	Observed
Unknown groups			
	[Interesting malware not linked to an actor yet]		

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=4b157100-22c4-4c04-83eb-245052a43b69>