Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:58:14 UTC

Tool: Shifu

Names	Shifu
Category	Malware
Type	Banking trojan, Credential stealer, Info stealer
Description	(Palo Alto) Shifu is a Banking Trojan first discovered in 2015. Shifu is based on the Shiz source code which incorporated techniques used by Zeus. Attackers use Shifu to steal credentials for online banking websites around the world, starting in Russia but later including the UK, Italy, and others. Palo Alto Networks Unit 42 research has found that the Shifu authors have evolved Shifu in 2016. Our research has found that Shifu has incorporated multiple new techniques to infect and evade detection on Microsoft Windows systems.
Information	<https://unit42.paloaltonetworks.com/unit42-2016-updates-shifu-banking-trojan/> <https://www.fireeye.com/blog/threat-research/2015/10/shifu-malware-analyzed-behavior-capabilities-and.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.shifu>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Shifu

Changed	Name	Country	Observed	
APT groups				
	Sprite Spider, Gold Dupont	[Unknown]	2015-Nov 2022	
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

2 groups listed (2 APT, 0 other, 0 unknown)
