Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:11:47 UTC

Tool: Farseer

Names	Farseer
Category	Malware
Type	Backdoor
Description	(Palo Alto) The threat actors behind Farseer, and related malware including HenBox, continue to grow their armoury with the addition of this previously-unknown malware family. The overlapping infrastructure, shared TTPs and similarities in malicious code and configurations highlights the web of threats used to target victims in and around the South East Asia region and perhaps beyond. Farseer payloads are backdoors that beacon to pre-configured C2 servers for instructions. The malware uses various techniques to evade detection and inhibit analysis. For example, DLL sideloading using trusted, signed executables allows the malware to execute rather seamlessly; some payloads are encrypted on disk preventing analysis, especially as decompression and decryption occurs at runtime, in-memory, where code is further altered to thwart forensic analysis. Whereas HenBox posed a threat for devices running Android, Farseer is built to target Windows, which appears to be more typical given previous threats seen from the group or groups behind this, and related malware.
Information	<https://unit42.paloaltonetworks.com/farseer-previously-unknown-malware-family-bolsters-the-chinese-armoury/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.farseer>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Farseer>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Farseer

Changed	Name	Country	Observed	
APT groups				
	Mustang Panda, Bronze President		2012-Jun 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3de28b40-0bda-4ae0-a87d-8e67085b5c7a