Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:35:33 UTC

Tool: Tofu Backdoor

Names	Tofu Backdoor
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Cylance) Based upon Cylance's observations, the Tofu Backdoor was deployed in far fewer instances than the Ham Backdoor. It is a proxy-aware, fully-featured backdoor programmed in C++ and compiled using Visual Studio 2015. The Tofu backdoor makes extensive use of threading to perform individual tasks within the code. It communicates with its C2 server through HTTP over nonstandard TCP ports, and will send encoded information containing basic system information back, including hostname, username, and operating system within the content of the POST.
Information	<https://threatvector.cylance.com/en_us/home/the-deception-project-a-new-japanese-centric-threat.html>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Tofu Backdoor

Changed	Name	Country	Observed	
APT groups				
	Snake Wine		2016	

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