Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:21:40 UTC

Tool: Saitama

Names	Saitama Saitama Backdoor AMATIAS
Category	Malware
Type	Backdoor
Description	(Malwarebytes) Saitama backdoor abuses the DNS protocol for its command and control communications. This is stealthier than other communication methods, such as HTTP. Also, the actor cleverly uses techniques such as compression and long random sleep times. They employed these tricks to disguise malicious traffic in between legitimate traffic.
Information	<https://blog.malwarebytes.com/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.saitama>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool Saitama

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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