Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:58:34 UTC

Tool: YamaBot

Names	YamaBot Kaos
Category	Malware
Type	Backdoor
Description	(JPCERT/CC) YamaBot malware communicates with C2 servers using HTTP requests. The following is a list of function names included in the sample that targets Windows OS. It is the attacker that named the malware as Yamabot. Those targeting Windows OS have functions specific to it, such as creating and checking Mutex.
Information	<https://blogs.jpcert.or.jp/en/2022/07/yamabot.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.yamabot>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool YamaBot

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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