Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:39:38 UTC

Tool: Taidoor

Names	Taidoor simbot
Category	Malware
Type	Backdoor
Description	(FireEye) The Taidoor malware is traditionally delivered as an email attachment. If opened, the Taidoor malware is dropped onto t
Information	<https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf> <http://contagiodump.blogspot.com/2011/10/sep-28-cve-2010-3333-manuscript-with.html> <https://www.nttsecurity.com/docs/librariesprovider3/resources/taidoor%E3%82%92%E7%94%A8%E3%81%84%E3%81%9F% <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a>
MITRE ATT&CK	<https://attack.mitre.org/software/S0011/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.taidoor>

Last change to this tool card: 04 August 2020

Download this tool card in JSON format

All groups using tool Taidoor

Changed	Name	Country	Observed	
APT groups				
	Taidoor		2008-Late 2015	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=91c4ec86-ad97-4e60-a6cb-415f28155d9b