Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:43:21 UTC

APT group: Taidoor

Names	Taidoor *(Trend Micro)* Budminer *(Symantec)* Earth Aughisky *(Trend Micro)* G0015 *(MITRE)*
Country	China
Motivation	Information theft and espionage
First seen	2008
Description	(Trend Micro) The Taidoor attackers have been actively engaging in targeted attacks since at least March 4, 2009. Despite some exceptions, the Taidoor campaign often used Taiwanese IP addresses as C&C servers and email addresses to send out socially engineered emails with malware as attachments. One of the primary targets of the Taidoor campaign appeared to be the Taiwanese government. The attackers spoofed Taiwanese government email addresses to send out socially engineered emails in the Chinese language that typically leveraged Taiwan-themed issues. The attackers actively sent out malicious documents and maintained several IP addresses for command and control. As part of their social engineering ploy, the Taidoor attackers attach a decoy document to their emails that, when opened, displays the contents of a legitimate document but executes a malicious payload in the background. We were only able to gather a limited amount of information regarding the Taidoor attackers' activities after they have compromised a target. We did, however, find that the Taidoor malware allowed attackers to operate an interactive shell on compromised computers and to upload and download files. In order to determine the operational capabilities of the attackers behind the Taidoor campaign, we monitored a compromised honeypot. The attackers issued out some basic commands in an attempt to map out the extent of the network compromise but quickly realized that the honeypot was not an intended targeted and so promptly disabled the Taidoor malware running on it. This indicated that while Taidoor malware were more widely distributed compared with those tied to other targeted campaigns, the attackers could quickly assess their targets and distinguish these from inadvertently compromised computers and honeypots.
Observed	Sectors: Government. Countries: Brazil, Japan, South Korea, Taiwan, USA.

Tools used	Dripion, Taidoor.	
Operations performed	Late 2015	Taiwan targeted with new cyberespionage back door Trojan <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b0649cc1-a60f-4cd7-ba3e-832e218de385&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf> <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/connecting-taidoors-dots-earth-aughisky-over-the-last-10-years>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0015/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
