GhostNet, Snooping Dragon - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:06:30 UTC

APT group: GhostNet, Snooping Dragon

Names	GhostNet *(Information Warfare Monitor)* Snooping Dragon *(UCAM)*
Country	China
Sponsor	State-sponsored, PLA Unit 61398
Motivation	Information theft and espionage
First seen	2009

Description	(Information Warfare Monitor) Cyber espionage is an issue whose time has come. In this second report from the Information Warfare Monitor, we lay out the findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions. The investigation, consisting of fieldwork, technical scouting, and laboratory analysis, discovered a lot more. The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information. (UCAM) Attacks on the Dalai Lama's Private Office The OHHDL started to suspect it was under surveillance while setting up meetings between His Holiness and foreign dignitaries. They sent an email invitation on behalf of His Holiness to a foreign diplomat, but before they could follow it up with a courtesy telephone call, the diplomat's office was contacted by the Chinese government and warned not to go ahead with the meeting. The Tibetans wondered whether a computer compromise might be the explanation; they called ONI Asia who called us. (Until May 2008, the first author was employed on a studentship funded by the OpenNet Initiative and the second author was a principal investigator for ONI.) Also see Shadow Network.	
Observed	Sectors: Embassies, Financial, Government, Media, NGOs. Countries: Bangladesh, Barbados, Bhutan, Brunei, Philippines, Cyprus, Germany, India, Indonesia, Iran, Latvia, Malta, Pakistan, Portugal, Romania, South Korea, Taiwan, Thailand, ASEAN, NATO and SAARC (South Asian Association for Regional Cooperation), the Asian Development Bank and news organizations.	
Tools used	Gh0stnet, Gh0st RAT, TOM-Skype.	
Counter operations	2010	Taken down by the Shadowserver Foundation.
Information	<http://www.nartv.org/mirror/ghostnet.pdf> <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf> <https://en.wikipedia.org/wiki/GhostNet>	

Last change to this card: 21 May 2021

Download this actor card in PDF or JSON format