Shadow Network - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:43:05 UTC

APT group: Shadow Network

Names	Shadow Network *(Information Warfare Monitor)*
Country	China
Motivation	Information theft and espionage
First seen	2010
Description	(Information Warfare Monitor) Shadows in the Cloud documents a complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. The report also contains an analysis of data which were stolen from politically sensitive targets and recovered during the course of the investigation. These include documents from the Offices of the Dalai Lama and agencies of the Indian national security establishment. Data containing sensitive information on citizens of numerous third-party countries, as well as personal, financial, and business information, were also exfiltrated and recovered during the course of the investigation. The report analyzes the malware ecosystem employed by the Shadows' attackers, which leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report is able to determine the location (Chengdu, PRC) as well as some of the associations of the attackers through circumstantial evidence. The investigation is the product of an eight month, collaborative activity between the Information Warfare Monitor (Citizen Lab and SecDev) and the Shadowserver Foundation. The investigation employed a fusion methodology, combining technical interrogation techniques, data analysis, and field research, to track and uncover the Shadow cyber espionage network. Also see GhostNet, Snooping Dragon.

Observed	Sectors: Education, Government and others. Countries: Afghanistan, Australia, Azerbaijan, Canada, China, France, Germany, Greece, Hong Kong, India, Israel, Italy, Japan, Lithuania, Malaysia, Mexico, Nepal, Netherlands, New Zealand, Pakistan, Papua New Guinea, Philippines, Qatar, Romania, Russia, South Korea, Sweden, Taiwan, Thailand, Tibet, UAE, UK, USA, Vietnam.	
Tools used	ShadowNet.	
Counter operations	2010	Taken down by the Shadowserver Foundation.
Information	<https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf>	

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
