Naikon, Lotus Panda - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:45:44 UTC

APT group: Naikon, Lotus Panda

Names	Naikon *(Kaspersky)* Hellsing *(Kaspersky)* Lotus Panda *(CrowdStrike)* ITG06 *(IBM)* G0019 *(MITRE)*	
Country	China	
Sponsor	State-sponsored, PLA Unit 78020	
Motivation	Information theft and espionage	
First seen	2010	
Description	Naikon is a threat group that has focused on targets around the South China Sea. The group has been attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). While Naikon shares some characteristics with APT 30, Override Panda, the two groups do not appear to be exact matches.	
Observed	Sectors: Defense, Energy, Government, Law enforcement, Media. Countries: Australia, Brunei, Cambodia, China, India, Indonesia, Laos, Malaysia, Myanmar, Nepal, Philippines, Saudi Arabia, Singapore, South Korea, Thailand, USA, Vietnam.	
Tools used	8.t Dropper, Aria-body, Aria-body loader, ARL, BackBend, Backspace, Creamsicle, Flashflood, FoundCore, Gemcutter, HDoor, JadeRAT, LadonGo, Milkmaid, Naikon, nbtscan, Nebulae, NetEagle, NewCore RAT, Orangeade, PlugX, Quarks PwDump, RARSTONE, Sandboxie, Shipshape, Sisfader, Spaceship, SslMM, Sys10, TeamViewer, Viper, WinMM, xsPlus, Living off the Land.	
Operations performed	2012	Naikon downloader/backdoor
	2013	"MsnMM" Campaigns <https://media.kasperskycontenthub.com/wp-

		content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf>
	Feb 2013	BKDR_RARSTONE RAT Last year, we reported about PlugX a breed of Remote Access Trojan (RAT) used in certain high-profile APT campaigns. We also noted some of its noteworthy techniques, which include its capability to hide its malicious codes by decrypting and loading a backdoor “executable file” directly into memory, without the need to drop the actual “executable file”. Recently, we uncovered a RAT using the same technique. The new sample detected by Trend Micro as BKDR_RARSTONE.A is similar (but not) PlugX, as it directly loads a backdoor “file” in memory without dropping any “file”. However, as we proceeded with our analysis, we found that BKDR_RARSTONE has some tricks of its own. <https://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/>
	Mar 2014	Campaign in the wake of the MH370 tragedy By March 11th, the Naikon group was actively hitting most of the nations involved in the search for MH370. The targets were extremely wide-ranging but included institutions with access to information related to the disappearance of MH370. <https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/>
	Sep 2015	Operation “CameraShy” <https://threatconnect.com/blog/camerashy-intro/>
	2017	Recently Check Point Research discovered new evidence of an ongoing cyber espionage operation against several national government entities in the Asia Pacific (APAC) region. This operation, which we were able to attribute to the Naikon APT group, used a new backdoor named Aria-body, in order to take control of the victims’ networks. <https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/>
	Apr 2022	The Lotus Panda is Awake, Again. Analysis of its Last Strike. <https://cluster25.io/2022/04/29/lotus-panda-awake-last-strike/>
Information	<https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/> <https://securelist.com/the-naikon-apt/69953/>	

	<https://exchange.xforce.ibmcloud.com/threat-group/guid:2f1962c4d7c0c994981c5bc363823c44>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0019/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
