Hidden Lynx, Aurora Panda - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Hidden Lynx, Aurora Panda

Names	Hidden Lynx *(Symantec)* Aurora Panda *(CrowdStrike)* Group 8 *(Talos)* Heart Typhoon *(Microsoft)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2009	
Description	(Symantec) The Hidden Lynx group has been in operation since at least 2009 and is most likely a professional organization that offers a “hackers for hire” service. They have the capability to attack many organizations with concurrently running campaigns. They operate efficiently and move quickly and methodically. Based on these fa Hidden Lynx group would need to be a sizeable organization made up of between 50 and 100 individuals. Much of the attack infrastructure and tools used during these campaigns originate from network infrastructure in The Hidden Lynx group makes regular use of zero-day exploits and has the ability to rework and customize explo quickly. They are methodical in their approach and they display a skillset far in advance of some other attack gro operating in that region, such as the Comment Crew (also known as APT1). The Hidden Lynx group is an advanc persistent threat that has been in operation for at least four years and is breaking into some of the best-protected organizations in the world. With a zero-day attack already under their belt in 2013, they continue to operate at the edge of targeted attacks. This group appears to be closely associated with APT 17, Deputy Dog, Elderwood, Sneaky Panda.	
Observed	Sectors: Construction, Defense, Education, Financial, Food and Agriculture, Engineering, Healthcare, IT, Goverr Media, Non-profit organizations, Pharmaceutical, Retail and lawyers. Countries: Australia, Canada, China, France, Germany, Hong Kong, India, Japan, Russia, Singapore, South Kore Taiwan, UK, Ukraine, USA.	
Tools used	BlackCoffee, HiKit, Moudoor, Naid.	
Operations performed	Jun 2012	VOHO campaign The VOHO campaign, first publicized by RSA, is one of the largest and most successful watering-h attacks to date. The campaign combined both regional and industry-specific attacks and predominan targeted organizations that operate in the United States. In a rapidly spreading two-phase attack, whi started on June 25 and finished July 18, nearly 4,000 machines had downloaded a malicious payloac payloads were being delivered to unsuspecting victims from legitimate websites that were strategica compromised. <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_
	Jul 2012	Breach of the Bit9 website <https://blog.bit9.com/2013/02/08/bit9-and-our-customers-security/>
Counter operations	2014	Operation “SMN” Security vendors take action against Hidden Lynx malware

		<https://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malwa
Information	<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf> <https://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire> <https://www.recordedfuture.com/hidden-lynx-analysis/>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
