SharpPanda, Sharp Dragon - Threat Group Cards: A Threat Actor Encyclopedia

APT group: SharpPanda, Sharp Dragon

Names	SharpPanda *(Check Point)* Sharp Dragon *(Check Point)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2018	
Description	(Check Point) Check Point Research identified an ongoing surveillance operation targeting a Southeast Asian government. The attackers use spear-phishing to gain initial access and leverage old Microsoft Office vulnerabilities together with the chain of in-memory loaders to attempt and install a previously unknown backdoor on victim's machines. Our investigation shows the operation was carried out by what we believe is a Chinese APT group that has been testing and refining the tools in its arsenal for at least 3 years.	
Observed	Sectors: Government. Countries: Indonesia, Malaysia, Thailand, Vietnam and Africa, the Caribbean and Southeast Asia.	
Tools used	8.t Dropper, Cobalt Strike.	
Operations performed	2024	Chinese Espionage Campaign Expands to Target Africa and The Caribbean <https://blog.checkpoint.com/research/chinese-espionage-campaign-expands-to-target-africa-and-the-caribbean/>
	Mar 2024	Inside the SharpPanda's Malware Targeting Malaysia <https://notes.netbytesec.com/2024/05/inside-sharppandas-malware-targeting.html>

Information	<https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/>

Last change to this card: 19 June 2024

Download this actor card in PDF or JSON format
