Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:06:46 UTC

APT group: Vicious Panda

Names	Vicious Panda *(Check Point)* Bronze Dudley *(SecureWorks)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2015	
Description	(Check Point) Check Point Research discovered a new campaign against the Mongolian public sector, which takes advantage of the current Coronavirus scare, in order to deliver a previously unknown malware implant to the target. A closer look at this campaign allowed us to tie it to other operations which were carried out by the same anonymous group, dating back to at least 2016. Over the years, these operations targeted different sectors in multiple countries, such as Ukraine, Russia, and Belarus.	
Observed	Sectors: Government. Countries: Belarus, Mongolia, Russia, Ukraine.	
Tools used	8.t Dropper, BBSRAT, Byeby, Cmstar, Enfal, Pylot.	
Operations performed	Aug 2015	Digital Quartermaster Scenario Demonstrated in Attacks Against the Mongolian Government <https://unit42.paloaltonetworks.com/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/>
	Jun 2017	Threat Actors Target Government of Belarus Using CMSTAR Trojan <https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan/>
	Mar 2020	Vicious Panda: The COVID Campaign Check Point Research discovered a new campaign against the Mongolian public sector, which takes advantage of the current Coronavirus scare, in order to deliver a previously unknown malware

		implant to the target. <https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/>
Information	<https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/>	

Last change to this card: 07 January 2021

Download this actor card in PDF or JSON format
