Threat Group Cards: A Threat Actor Encyclopedia

APT group: UNC4191

Names	UNC4191 *(Mandiant)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(Mandiant) Mandiant Managed Defense recently identified cyber espionage activity that heavily leverages USB devices as an initial infection vector and concentrates on the Philippines. Mandiant tracks this activity as UNC4191 and we assess it has a China nexus. UNC4191 operations have affected a range of public and private sector entities primarily in Southeast Asia and extending to the U.S., Europe, and APJ; however, even when targeted organizations were based in other locations, the specific systems targeted by UNC4191 were also found to be physically located in the Philippines.
Observed	Countries: Philippines.
Tools used	BLUEHAZE, DARKDEW, MISTCLOAK, NCAT.
Information	<https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia> <https://therecord.media/espionage-group-using-usb-devices-to-hack-targets-in-southeast-asia>

Last change to this card: 12 March 2024

Download this actor card in PDF or JSON format
