Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:32:20 UTC

APT group: Earth Wendigo

Names	Earth Wendigo *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2019
Description	(Trend Micro) We discovered a new campaign that has been targeting several organizations — including government organizations, research institutions and universities in Taiwan — since May 2019, aiming to exfiltrate emails from targeted organizations via the injection of JavaScript backdoors to a webmail system that is widely-used in Taiwan. With no clear connection to any previous attack group, we gave this new threat actor the name “Earth Wendigo.” Additional investigation shows that the threat actor also sent spear-phishing emails embedded with malicious links to multiple individuals, including politicians and activists, who support movements in Tibet, the Uyghur region, or Hong Kong. However, this is a separate series of attacks from their operation in Taiwan, which this report covers.
Observed	Sectors: Education, Government and politicians and activists, who support movements in Tibet, the Uyghur region, or Hong Kong. Countries: Taiwan.
Tools used	Cobalt Strike.
Information	<https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html>

Last change to this card: 07 January 2021

Download this actor card in PDF or JSON format