Threat Group Cards: A Threat Actor Encyclopedia

APT group: CardinalLizard

Names	CardinalLizard *(Kaspersky)*
Country	China
Motivation	Information theft and espionage
First seen	2014
Description	(Kaspersky) We are moderately confident that this is a new collection of Chinese-speaking activity targeting businesses, active since 2014. Over the last few years, the group has shown an interest in the Philippines, Russia, Mongolia and Malaysia, the latter especially prevalent during 2018. The hackers use a custom malware featuring some interesting anti-detection and anti-emulation techniques. The infrastructure used also shows some overlaps with Roaming Tiger and previous PlugX campaigns, but this could just be due to infrastructure reuse under the Chinese-speaking umbrella.
Observed	Countries: Malaysia, Mongolia, Philippines, Russia.
Tools used	PlugX.
Information	<https://securelist.com/apt-trends-report-q1-2018/85280/>

Last change to this card: 29 April 2020

Download this actor card in PDF or JSON format