Operation Jacana - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:35:58 UTC

APT group: Operation Jacana

Names	Operation Jacana *(ESET)*
Country	China
Motivation	Information theft and espionage
First seen	2023
Description	(ESET) In February 2023, ESET researchers detected a spearphishing campaign targeting a governmental entity in Guyana. While we haven't been able to link the campaign, which we named Operation Jacana, to any specific APT group, we believe with medium confidence that a China-aligned threat group is behind this incident. In the attack, the operators used a previously undocumented C++ backdoor that can exfiltrate files, manipulate Windows registry keys, execute CMD commands, and more. We named the backdoor DinodasRAT based on the victim identifier it sends to its C&C: the string always begins with Din, which reminded us of the hobbit Dinodas from the Lord of the Rings.
Observed	Countries: Guyana.
Tools used	DinodasRAT, Impacket, PlugX, SoftEther VPN.
Information	<https://www.welivesecurity.com/en/eset-research/operation-jacana-spying-guyana-entity/>

Last change to this card: 13 October 2023

Download this actor card in PDF or JSON format