Snake Wine - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:39:40 UTC

APT group: Snake Wine

Names	Snake Wine *(Cylance)*
Country	China
Motivation	Information theft and espionage
First seen	2016
Description	(Cylance) While investigating some of the smaller name servers that Sofacy, APT 28, Fancy Bear, Sednit routinely use to host their infrastructure, Cylance discovered another prolonged campaign that appeared to exclusively target Japanese companies and individuals that began around August 2016. The later registration style was eerily close to previously registered APT28 domains, however, the malware used in the attacks did not seem to line up at all. During the course of our investigation, JPCERT published this analysis of one of the group's backdoors. Cylance tracks this threat group internally as 'Snake Wine'. The Snake Wine group has proven to be highly adaptable and has continued to adopt new tactics in order to establish footholds inside victim environments. The exclusive interest in Japanese government, education, and commerce will likely continue into the future as the group is just starting to build and utilize their existing current attack infrastructure.
Observed	Sectors: Education, Government and Commerce. Countries: Japan.
Tools used	ChChes, Tofu Backdoor.
Information	<https://threatvector.cylance.com/en_us/home/the-deception-project-a-new-japanese-centric-threat.html> <https://www.jpcert.or.jp/magazine/acreport-ChChes.html>

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format