Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:07:06 UTC

APT group: ShaggyPanther

Names	ShaggyPanther *(Kaspersky)*
Country	China
Motivation	Information theft and espionage
First seen	2018
Description	(Kaspersky) We first discussed ShaggyPanther, a previously unseen malware and intrusion set targeting Taiwan and Malaysia, in a private report in January 2018. Related activities date back to more than a decade ago, with similar code maintaining compilation timestamps from 2004. Since then, ShaggyPanther activity has been detected in several more locations: most recently in Indonesia in July, and – somewhat surprisingly – in Syria in March. The newer 2018 and 2019 backdoor code maintains a new layer of obfuscation and no longer maintains clear-text C2 strings. Since our original release, we have identified an initial server-side infection vector from this actor, using SinoChopper/ChinaChopper, a commonly used web shell shared by multiple Chinese-speaking actors. SinoChopper not only performs host identification and backdoor delivery but also email archive theft and additional activity. Although not all incidents can be traced back to server-side exploitation, we did detect a couple of cases and obtained information about their staged install process. In 2019, we observed ShaggyPanther targeting Windows servers.
Observed	Sectors: Government. Countries: Indonesia, Malaysia, Syria, Taiwan.
Tools used	China Chopper.
Information	<https://securelist.com/ksb-2019-review-of-the-year/95394/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format