Operation Silent Skimmer - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:10:39 UTC

APT group: Operation Silent Skimmer

Names	Operation Silent Skimmer *(BlackBerry)*
Country	[Unknown]
Motivation	Financial crime
First seen	2022
Description	(BlackBerry) BlackBerry has discovered a new campaign we've dubbed "Silent Skimmer," involving a financially motivated threat actor targeting vulnerable online payment businesses in the APAC and NALA regions. The attacker compromises web servers, using vulnerabilities to gain initial access. The final payload deploys payment scraping mechanisms on compromised websites to extract sensitive financial data from users. The campaign has been active for over a year, and targets diverse industries that host or create payment infrastructure, such as online businesses and Point of Sales (POS) providers. We have uncovered evidence suggesting the threat actor is proficient in the Chinese language, and operates predominantly in the Asia-Pacific (APAC) region.
Observed	Countries: USA and Asia Pacific.
Tools used	BadPotato, Cobalt Strike, GodPotato, Godzilla, JuicyPotato, PowerShell RAT, SharpToken, SweetPotato, Living off the Land.
Information	<https://blogs.blackberry.com/en/2023/09/silent-skimmer-online-payment-scraping-campaign-shifts-targets-from-apac-to-nala>

Last change to this card: 12 October 2023

Download this actor card in PDF or JSON format