Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:57:51 UTC

APT group: Carderbee

Names	Carderbee *(Symantec)*
Country	China
Motivation	Information theft and espionage
First seen	2023
Description	(Symantec) A previously unknown advanced persistent threat (APT) group used the legitimate Cobra DocGuard software to carry out a supply chain attack with the goal of deploying the Korplug backdoor (aka PlugX) onto victim computers. In the course of this attack, the attackers used malware signed with a legitimate Microsoft certificate. Most of the victims in this campaign are based in Hong Kong, with some victims based in other regions of Asia. Korplug is known to be used by multiple APT groups, but we could not link this activity to a known threat actor so we have given the actor behind this activity a new name — Carderbee.
Observed	Countries: Hong Kong and Asia.
Tools used	Cobra DocGuard, PlugX.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse>

Last change to this card: 06 September 2023

Download this actor card in PDF or JSON format
