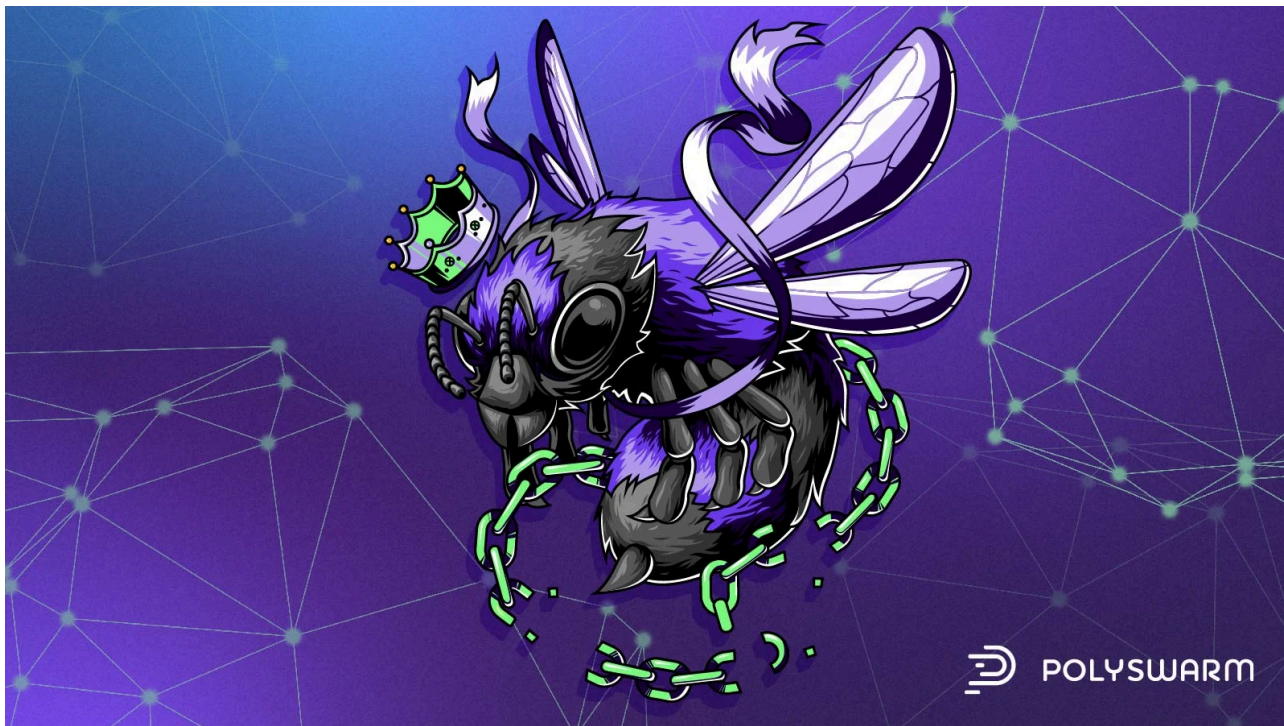


Carderbee Targets Hong Kong in Supply Chain Attack

By The Hivemind

Archived: 2026-04-02 10:40:55 UTC

Sep 8, 2023 2:29:33 PM / by [The Hivemind](#)



Related Families: Korplug, PlugX

Executive Summary

In a recent campaign, Carderbee targeted entities in Hong Kong and other regions of Asia via a supply chain attack leveraging the legitimate Cobra DocGuard software.

Key Takeaways

- A recent campaign targeted entities in Hong Kong and other regions of Asia via a supply chain attack leveraging the legitimate Cobra DocGuard software.
- The threat actors targeted these entities with the goal of deploying a version of Korplug (PlugX) on victim systems.
- Some of the malware used in the campaign was signed with a Microsoft certificate.
- Symantec attributed this activity to a previously unnamed group they dubbed Carderbee.

The Campaign

Symantec recently [reported](#) on activity attributed to a threat actor group dubbed Carderbee. In the campaign, the threat actors target entities in Hong Kong and other regions of Asia via a supply chain attack leveraging the legitimate Cobra DocGuard software. The activity began as early as September 2022.

The threat actors targeted these entities with the goal of deploying a version of Korplug (PlugX) on victim systems. The version of Korplug used had multiple capabilities including executing commands via CMD, enumerating files, checking running processes, downloading files, opening firewall ports, and keylogging. Some of the malware used in the campaign was signed with a Microsoft certificate. While over 2000 computers were affected by the Cobra DocGuard software used in the campaign, only about 100 had evidence of malicious activity. This likely indicates that Carderbee was selectively targeting certain entities.

Who is Carderbee?

Cobra DocGuard, legitimate encryption software, has been previously used by China nexus threat actor groups including Winnti and Budworm. Since the other TTPs did not seem to follow those of a known threat actor group, Symantec attributed this activity to a previously unnamed group they dubbed Carderbee. Symantec noted that Carderbee appears to consist of patient and skilled threat actors. At this time, no other details about the threat actor group are available.

IOCs

PolySwarm has multiple samples associated with this activity.

[B5159f8ae16deda7aa5d55100a0eac6e5dacd1f6502689b543513a742353d1ea](#)

[96170614bbd02223dc79cec12afb6b11004c8edb8f3de91f78a6fc54d0844622](#)

[2400d8e66c652f4f8a13c99a5ffb67cb5c0510144b30e93122b1809b58614936](#)

[7e6d0f14302662f52e4379eb5b69a3749d8597e8f61266aeda74611258972a3d](#)

[1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d](#)

[f64267decaa982c63185d92e028f52c31c036e85b2731a6e0bccdb8f7b646e97](#)

You can use the following CLI command to search for all related samples in our portal:

\$ polyswarm link list -f Carderbee

Don't have a PolySwarm account? Go [here](#) to sign up for a free Community plan or to subscribe.

Contact us at hivemind@polyswarm.io | Check out our [blog](#) | [Subscribe](#) to our reports