Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:48:02 UTC

APT group: Bookworm

Names	Bookworm *(Palo Alto)*
Country	China
Motivation	Information theft and espionage
First seen	2015
Description	(Palo Alto) Threat actors have delivered Bookworm as a payload in attacks on targets in Thailand. Readers who are interested in this campaign should start with our first blog that lays out the overall functionality of the malware and introduces its many components. Unit 42 does not have detailed targeting information for all known Bookworm samples, but we are aware of attempted attacks on at least two branches of government in Thailand. We speculate that other attacks delivering Bookworm were also targeting organizations in Thailand based on the contents of the associated decoys documents, as well as several of the dynamic DNS domain names used to host C2 servers that contain the words “Thai” or “Thailand”. Analysis of compromised systems seen communicating with Bookworm C2 servers also confirms our speculation on targeting with a majority of systems existing within Thailand.
Observed	Sectors: Defense, Government. Countries: Thailand.
Tools used	Bookworm, FormerFirstRAT, Poison Ivy, PlugX, Scieron.
Information	<https://unit42.paloaltonetworks.com/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/> <https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format