Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:36:46 UTC

Tool: Bookworm

Names	Bookworm
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	(Palo Alto) Bookworm's functional code is radically different from PlugX and has a rather unique modular architecture that warranted additional analysis by Unit 42. Bookworm has little malicious functionality built-in, with its only core ability involving stealing keystrokes and clipboard contents. However, Bookworm expands on its capabilities through its ability to load additional modules directly from its command and control (C2) server.
Information	<https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bookworm>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool Bookworm

Changed	Name	Country	Observed	
APT groups				
	Bookworm		2015	

1 group listed (1 APT, 0 other, 0 unknown)