Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:34:22 UTC

APT group: Operation PseudoManuscrypt

Names	Operation PseudoManuscrypt *(Kaspersky)*
Country	China
Motivation	Information theft and espionage
First seen	2021
Description	(Kaspersky) In June 2021, Kaspersky ICS CERT experts identified malware whose loader has some similarities to the Manuscrypt malware, which is part of the Lazarus Group, Hidden Cobra, Labyrinth Chollima APT group's arsenal. In 2020, the group used Manuscrypt in attacks on defense enterprises in different countries. These attacks are described in the report "Lazarus targets defense industry with ThreatNeedle". Curiously, the data exfiltration channel of the malware uses an implementation of the KCP protocol that has previously been seen in the wild only as part of the APT 41 group's toolset. We dubbed the newly-identified malware PseudoManuscrypt. The PseudoManuscrypt loader makes its way onto user systems via a MaaS platform that distributes malware in pirated software installer archives. One specific case of the PseudoManuscrypt downloader's distribution is its installation via the Glupteba botnet (whose main installer is also distributed via the pirated software installer distribution platform). This means that the malware distribution tactics used by the threat actor behind PseudoManuscrypt demonstrate no particular targeting. During the period from January 20 to November 10, 2021, Kaspersky products blocked PseudoManuscrypt on more than 35,000 computers in 195 countries of the world. Such a large number of attacked systems is not characteristic of the Lazarus group or APT attacks as a whole. Targets of PseudoManuscrypt attacks include a significant number of industrial and government organizations, including enterprises in the military-industrial complex and research laboratories.

Observed	Sectors: Construction, Defense, Energy, Engineering, Government, Industrial, Manufacturing, Utilities. Countries: Worldwide.
Tools used	PseudoManuscrypt.
Information	<https://ics-cert.kaspersky.com/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/>

Last change to this card: 27 December 2021

Download this actor card in PDF or JSON format
