# PseudoManuscrypt: a mass-scale spyware attack campaign

securelist.com/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/105286/

Industrial threats

Industrial threats

16 Dec 2021

minute read

Authors

Expert Kaspersky ICS CERT

In June 2021, Kaspersky ICS CERT experts identified malware whose loader has some similarities to the Manuscrypt malware, which is part of the Lazarus 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 APT41 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.

According to our telemetry, at least 7.2% of all computers attacked by the PseudoManuscrypt malware are part of industrial control systems (ICS) used by organizations in various industries, including Engineering, Building Automation, Energy, Manufacturing, Construction, Utilities, and Water Management.

The main PseudoManuscrypt module has extensive and varied spying functionality. It includes stealing VPN connection data, logging keypresses, capturing screenshots and videos of the screen, recording sound with the microphone, stealing clipboard data and operating system event log data (which also makes stealing RDP authentication data possible), and much more. Essentially, the functionality of PseudoManuscrypt provides the attackers with virtually full control of the infected system.

More information on PseudoManuscrypt is available on the Kaspersky ICS CERT website.

- Data theft
- Industrial control systems
- Lazarus
- Malware Descriptions
- Malware Statistics
- Malware Technologies
- Phishing
- Spyware

Authors


Kaspersky ICS CERT

PseudoManuscrypt: a mass-scale spyware attack campaign

---

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

## GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

## Threat landscape for industrial automation systems, H2 2021

## Threat landscape for industrial automation systems in H1 2021

## Threat landscape for industrial automation systems. Statistics for H2 2020

## Threat landscape for industrial automation systems. H1 2020 highlights

## Threat Landscape for Industrial Automation Systems in H2 2018

Subscribe to our weekly e-mails

The hottest research right in your inbox

-

Reports

## APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

## Lazarus Trojanized DeFi app for delivering malware

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

## MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

## The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.