Careers

W/ Labs™

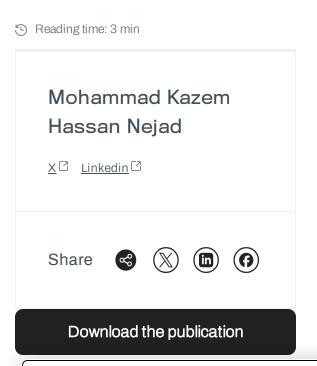
Research

**Expertise** 

Tools

Advisories

**Contact Us** 

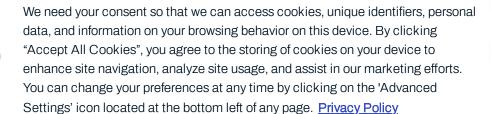


WithSecure has uncovered a novel backdoor that has been used in attacks against victims in Eastern Europe since at least mid-2022.

The malware, which we are calling "Kapeka", is a flexible backdoor with all the necessary functionalities to serve as an

parly-etage toolkit for its operators, and also to provide long-

## We value your privacy



Accept All Cookies

Reject All

Advanced Settings

λll

ure

state threat group operated by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). Sandworm is particularly notorious for its destructive attacks against Ukraine in pursuit of Russian interests in the region.

Kapeka contains a dropper that will drop and launch a backdoor on a victim's machine and then remove itself. The backdoor will first collect information and fingerprint both the machine and user before sending the details on to the threat actor. This allows tasks to be passed back to the machine or the backdoor's configuration to be updated. WithSecure do not have insight as to how the Kapeka backdoor is propagated by Sandworm.

Kapeka's development and deployment likely follow the ongoing Russia-Ukraine conflict, with Kapeka being likely used in targeted attacks of firms across Central and Eastern Europe since the illegal invasion of Ukraine in 2022.

It is likely that Kapeka was used in intrusions that led to the deployment of Prestige ransomware in late 2022. It is probable that Kapeka is a successor to GreyEnergy, which itself was likely a replacement for BlackEnergy in Sandworm's arsenal.

This report provides an in-depth technical analysis of the backdoor and its capabilities, and analyzes the connection between Kapeka and Sandworm group. The purpose of this report is to raise awareness amongst businesses, governments, and the broader security community. WithSecure has engaged governments and select customers with advanced copies of this report. In addition to the report, we are releasing several artifacts developed as a result of our research, including a registry-based & hardcoded configuration extractor, a script to decrypt and emulate the backdoor's network communication, and as might be expected, a list of indicators of compromise, YARA rules, and MITRE ATT&CK mapping.

23.04.2024 - Design and formatting of the report have been updated. Figure 37 has been updated as well to more clearly represent our understanding of the links between events.

## We value your privacy

With Resp We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. Privacy Policy

in X

0

© WithSecure 2024

Vulnerability Disclosure Policy

WithSecure™ Labs Publications

## We value your privacy

We need your consent so that we can access cookies, unique identifiers, personal data, and information on your browsing behavior on this device. By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. You can change your preferences at any time by clicking on the 'Advanced Settings' icon located at the bottom left of any page. Privacy Policy