# Twisted Panda: Chinese APT Launch Spy Operation Against Russian Defence Institutes

gbhackers.com/twisted-panda-chinese-apt/

May 24, 2022


In an analysis published recently by specialists at Check Point Research, a new spy campaign was discovered, dubbed “Twisted Panda”. This spy operation primarily targeted two Russian defense institutes and a research facility in Belarus.

In the course of an ongoing espionage campaign that has been taking place for several months, this campaign forms part of a larger, Chinese state-sponsored operation.

A variety of malicious stages and payloads have been deployed by the threat actors in this campaign. Moreover, there are also phishing emails containing sanctions-related information that has been sent to Russian entities within the Rostec Corporation, a Russian defense conglomerate.

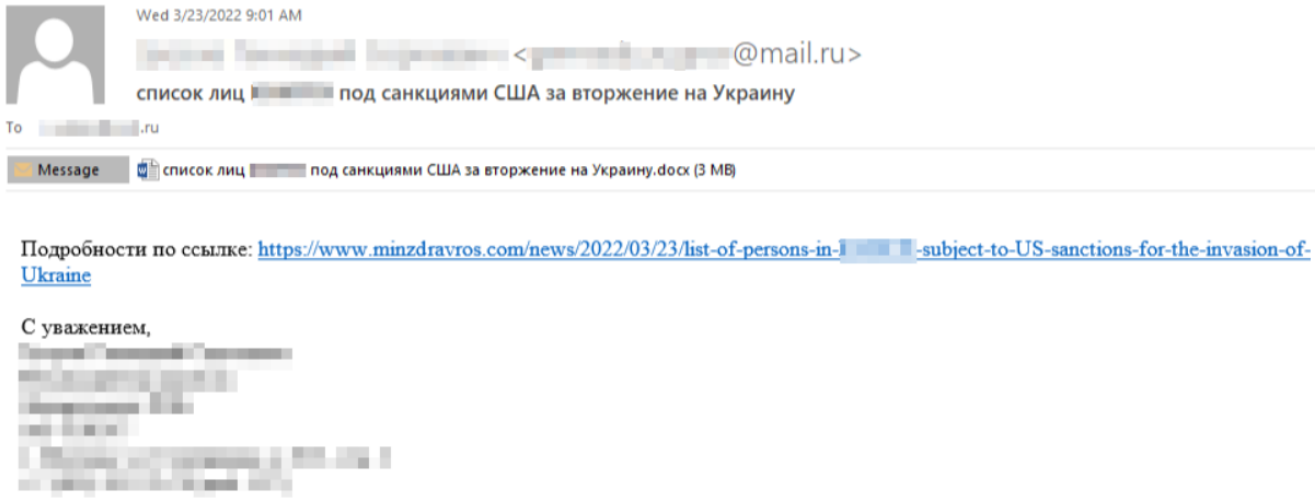
The invasion of Ukraine was exploited by another Chinese APT group, Mustang Panda, to target Russian organizations at the same time.

It is possible that Twisted Panda is a part of the same spy ring as Mustang Panda or Stone Panda, aka APT10, another Beijing-sponsored spy group.

## Infection chain

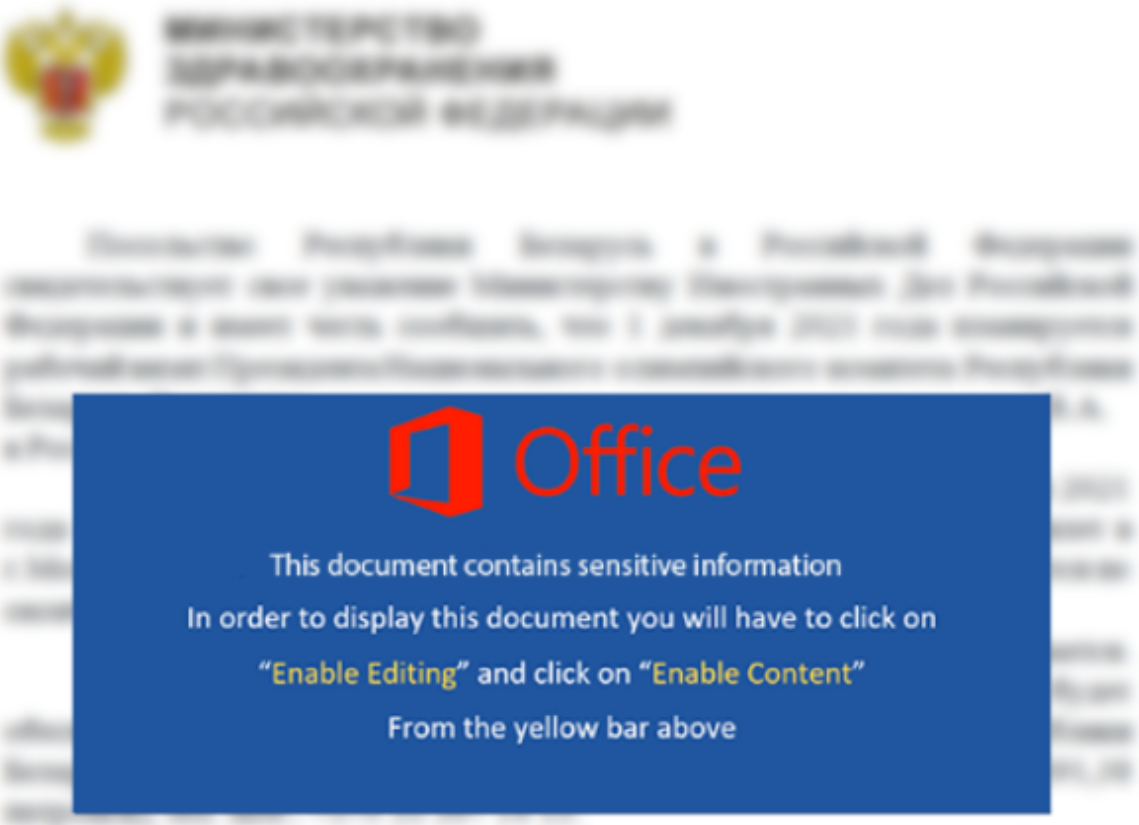
As recently on March 23, several Russian research institutes affiliated with the defense industry received malicious emails.

A malicious document was attached to the emails with the subject “List of persons under US sanctions for invading Ukraine”, which could be accessed through a link to a fake Russian Health Ministry website minzdravros[.]com.

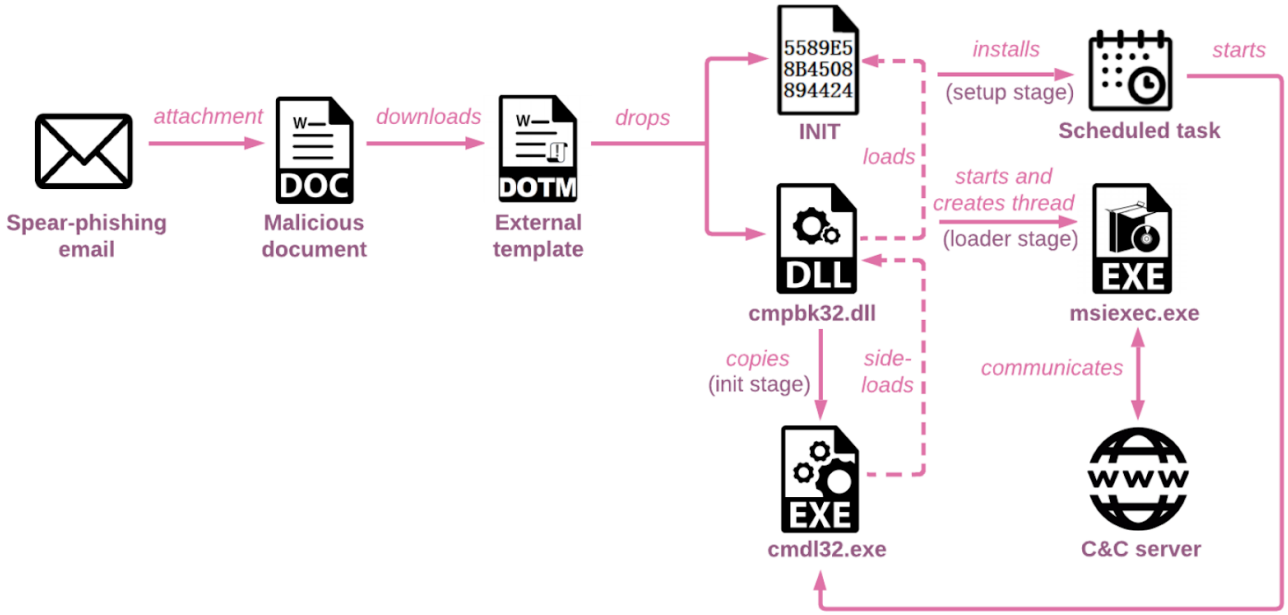



An email with the subject “US Spread of Deadly Pathogens in Belarus” was sent to an unknown entity in Minsk, Belarus on the same day.

While all of the documents attached to this email are crafted to appear to be official documents, bearing the official emblems and titles of the Russian Ministry of Health.




A template is downloaded from the URLs for each document in a similar format that can be easily exported. Several API functions are imported into this external template from kernel32, through a macro code.




When the exported function R1 is executed, the malicious files are finalized after initialization by the exported program.

## New Spinner backdoor

As the payload, the Spinner a newly added backdoor is the main component, which is obfuscated by using two methods of obfuscation.

It has been seen that earlier samples attributed to Stone Panda and Mustang Panda attested to the combination of these two obfuscation methods.

There are two major problems, and here they are:-

- Control-flow flattening: Which makes the code flow not linear.
- Opaque predicates: Which causes unneeded calculations to be performed in the binary.

In this case, Spinner is the backdoor used by a command-and-control server for the purpose of running additional payloads.

China's five-year plan also identifies Twisted Panda as part of its effort to improve its scientific and technological capabilities.

## Leave a Reply