Cyber attacks:
Igor GARSHIN

PERSONAL DETAILS

Family name: GARSHIN

First names: Igor

Date of birth: 02.12.1991

Place of birth: Tschita/Russia

Nationality: Russian

DESCRIPTION

Height: 180 cm

Appearance: Dark blonde hair and brown eyes

Languages: russian

SUMMARY OF THE FACTS OF THE CASE/CHARGES

Igor GARSHIN (alternative spelling: GARSCHIN) is suspected of having acted as one of the principal offenders in the commission of several cyberattacks on German companies. Specifically, it has been proven that the wanted person was significantly involved in the attacks by spying out, infiltrating and finally encrypting the data of the prejudiced companies.

The investigations have revealed that the cyberattacks in question can be attributed to the group "Indrik Spider", also known as "Doppel Spider". The first known attack committed by "Indrik Spider" was directed against the National Health Service of the United Kingdom in 2017. The offenders used ransomware called BitPaymer for this attack.

BitPaymer is an encryption trojan ransomware. Following infiltration, data are exfiltrated in a first step and the data files stored in the system are then encrypted by the software. The victims are subsequently asked to pay ransom money in exchange for access to their data. In many cases, funds in the double-digit million range were thus extorted from more than 600 victims throughout the world.

As from 2019, the group increasingly came to notice in connection with the ransomware DoppelPaymer, changed the name to PayOrGrief in 2021 and again to Entropy in January 2022.

The wanted person is therefore suspected of complicity in attempted extortion as well as computer sabotage, each time in especially serious cases, and of being a member of the criminal group "Indrik Spider“ / “Doppel Spider".

It is assumed that the wanted person may be living in the city of Yoshkar-Ola in Russia.

The wanted person's current whereabouts are unknown.

INFORMATION WANTED

Have you seen GARSHIN after 28 February 2023?

Can you provide information on the wanted person's current whereabouts?

Do you have information indicating that the wanted person travelled outside the Russian Federation?

Were or are you in contact with the wanted person?

Do you have information on current websites hosted by the wanted persons or any means of communication presently used?

OFFICE IN CHARGE OF THIS CASE

Land Criminal Police Office of North Rhine Westphalia

Special task Cybercrime

Völklingerstr. 49

40221 Düsseldorf

Germany

E-Mail: OPParker.LKA@polizei.nrw.de