SBU blocks activity of transnational hacking group

ssu.gov.ua/en/novyny/sbu-zablokuvala-diialnist-transnatsionalnoho-khakerskoho-uhrupovannia

The SBU cyber specialists blocked activity of a transnational criminal hacker group. The operation was conducted in the framework of international cooperation with the United States and France.

The SBU cyber specialists documented that since September 2020, these hackers have affected more than 150 companies in Europe and the United States. The companies' losses are more than USD 80 m.

During the cyber investigation, the SBU officers established that a group of people operating in Ukraine used Egregor malicious software.

With its help the offenders:

• encrypted computer networks of foreign companies,

• stole personal data of companies' customers and employees,

• stole information about financial indicators and technological developments,

• blocked the work of web resources.

The perpetrators demanded large sums of money, mostly in cryptocurrency, for decrypting the affected computer networks and not disclosing the stolen confidential data.

In February 2021, law enforcement officers stopped the illegal activity. During the investigation, computer equipment with the Egregor virus, information about the affected computer networks and other evidence of illegal activity were seized.

The members of the hacker group, including the organizer, were served a notice suspicion of committing criminal offenses of extortion, unauthorized interference in the work of computers, automated systems, computer or telecommunication networks.

The investigation is ongoing.

The operation was conducted under supervision of Kyiv Local Prosecutor's Office No.1.

ATTENTION!

Because of the liquidation of the transnational hacker group that operated using the extortion virus "Egregor" we appeal to the foreign competent law enforcement bodies that have enough information about the affected foreign companies to contact the Security Service of

Ukraine via e-mail dkib@ssu.gov.ua or by mail to the SSU address: 01601, Kyiv, 33, Volodymyrska Street, CyberSecurity (DKIB) department of the Security Service of Ukraine.