The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

EU Sanctions Russian, Chinese 'Cyber Attackers'

By Dave Clark for AFP

July 30, 2020

A unit of Moscow's GRU military intelligence agency is accused of cyber attacks on EU private companies. **Kyle Wagaman / Flickr (CC BY-NC-ND 2.0)**

The European Union imposed its first ever sanctions against alleged cyber attackers on Thursday, targeting Russian and Chinese individuals and a specialist unit of Moscow's GRU military intelligence agency.

An export firm based in North Korea and technology company from Tiajin, China, were also listed.

Related article: EU Considers Sanctions Against Chinese, Russian Groups Over Hacking

The member states said measures would be taken against six individuals and three entities involved in various actions, including the attempt to hack into the Organization for the

Prohibition of Chemical Weapons (OPCW).

They also included suspects said to be involved in the major cyber assaults known by the nicknames "WannaCry," "NotPetya" and "Operation Could Hopper."

The individuals will be banned from travel to the European Union and all the targets will be subject to an asset freeze for any funds in areas under EU jurisdiction.

In addition, the European Council of member states said: "EU persons and entities are forbidden from making funds available to those listed."

EU foreign policy chief Josep Borrell said the action had been taken "to better prevent, discourage, deter and respond to such malicious behavior in cyberspace."

These attacks, he said, represented "an external threat to the European Union or its member states" or had "a significant effect against third States or international organizations."

The best known of the targeted entities is the Main Center for Special Technologies, a unit of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation — better known as the GRU.

This unit, based on Kirova Street in Moscow, is said to have carried out attacks known as NotPetya and EternalPetya in June 2017, hitting EU private companies with ransomware and blocking data.

The sanctions list also accuses GRU agents of carrying out an attack on the Ukrainian power grid in the winters of 2015 and 2016, resulting in parts of it being shut down.

Four alleged Russian GRU agents — two "human intelligence support" officers and two "cyber operators" — are also named, for their roles in the April 2018 attempt to penetrate the OPCW agency in The Hague.

The watchdog was investigating reports that Russian-backed Syrian forces carried out chemical attacks when alleged GRU agents were intercepted trying to penetrate the agency's wifi from a hire car parked near its headquarters.

"With these sanctions, the EU is taking a big step towards safer cyber space. The price for bad behavior is being increased, because the bad guys still get away with it too often," said Dutch foreign minister Stef Blok.

"Now the EU shows that it can take effective action against these and other malicious parties," he said.

The other two entities targeted were Tianjin Huaying Haitai Science and Technology Development Company Ltd, said to be the actor known to cyber war observers as "Advanced Persistent Threat 10" or APT10.

Haitai is said to have been the source of "Operation Cloud Hopper," which the European Council said "targeted information systems of multinational companies in six continents ... and gained unauthorised access to commercially sensitive data, resulting in significant

economic loss."

Another target was Chosun Expo, an export company from North Korea which, under the "WannaCry" banner, is said to have helped hack the Polish Financial Supervision Authority and Sony Pictures Entertainment.

It is alleged to have carried out cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank.