Office of Financial
Sanctions Implementation
HM Treasury

Financial Sanctions Notice

31/07/2020

Cyber-Attacks

Introduction

1. Council Regulation (EU) 2019/796 ("the Regulation") imposing financial sanctions against Cyber-Attacks has been amended so that an asset freeze now applies to the persons listed in the Annex to this Notice.

Notice summary (Full details are provided in the Annex to this Notice)

2. The 9 entries listed in the Annex to this notice have been added to the consolidated list and are now subject to an asset freeze.

What you must do

3. You must:

   i. check whether you maintain any accounts or hold any funds or economic resources for the persons set out in the Annex to this Notice;

   ii. freeze such accounts, and other funds or economic resources;

   iii. refrain from dealing with the funds or assets or making them available (directly or indirectly) to such persons unless licensed by the Office of Financial Sanctions Implementation (OFSI);

   iv. report any findings to OFSI, together with any additional information that would facilitate compliance with the Regulation;

v. provide any information concerning the frozen assets of designated persons that OFSI may request. Information reported to OFSI may be passed on to other regulatory authorities or law enforcement.

4. Failure to comply with financial sanctions legislation or to seek to circumvent its provisions is a criminal offence.

Legislative details

5. On 30 July 2020 Council Implementing Regulation (EU) 2020/1125 ("the Amending Regulation") was published in the Official Journal of the European Union (O.J. L 246, 30.7.2020, p.4) by the Council of the European Union.

6. The Amending Regulation amended Annex I to the Regulation with effect from 30 July 2020.

Further Information

7. A copy of the Amending Regulation can be obtained from the website of the Official Journal of the European Union:

   https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1125&from=EN

8. Copies of recent Notices, certain EU Regulations, and UK legislation can be obtained from the Cyber-Attacks financial sanctions page on the GOV.UK website:

   https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

9. For more information please see our guide to financial sanctions:
   https://www.gov.uk/government/publications/financial-sanctions-faqs

Enquiries

10. Non-media enquiries, reports and licence applications should be addressed to:

    Office of Financial Sanctions Implementation
    HM Treasury
    1 Horse Guards Road
    London
    SW1A 2HQ
    ofsi@hmtreasury.gov.uk

11. Media enquiries about how financial sanctions are implemented in the UK should be addressed to the Treasury Press Office on 020 7270 5238.

12. Media enquiries about the sanctions measures themselves should be addressed to the Foreign and Commonwealth Office Press Office on 020 7008 3100.

ANNEX TO NOTICE

FINANCIAL SANCTIONS: CYBER-ATTACKS

COUNCIL IMPLEMENTING REGULATION (EU) 2020/1125

AMENDING ANNEX I TO COUNCIL REGULATION (EU) 2019/796

ADDITIONS

Individuals

1. **GAO, Qiang**
   POB: Shandong Province, China **Nationality:** Chinese **Address:** Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China. **Other Information:** Gender: male. Gao Qiang is involved in "Operation Cloud Hopper", a series of cyber-attacks. "Operation Cloud Hopper" targeted information systems of multinational companies in six continents, including companies located in the European Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as "APT10" ("Advanced Persistent Threat 10") (a.k.a. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" and "Potassium") carried out "Operation Cloud Hopper". Gao Qiang can be linked to APT10, including through his association with APT10 command and control infrastructure. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating "Operation Cloud Hopper", employed Gao Qiang. He has links with Zhang Shilong, who is also designated in connection with "Operation Cloud Hopper". Gao Qiang is therefore associated with both Huaying Haitai and Zhang Shilong. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13903.

2. **MININ, Alexey Valeryevich**
   DOB: 27/05/1972. **POB:** Perm Oblast, Russian SFSR (now Russian Federation) **Nationality:** Russian **Passport Details:** 120017582. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022 **Address**: Moscow, Russian Federation. **Other Information:** Gender: male. Alexey Minin took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Alexey Minin was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13905.

3. **MORENETS, Aleksei Sergeyvich**
   DOB: 31/07/1977. **POB:** Murmanskaya Oblast, Russian SFSR (now Russian Federation) **Nationality:** Russian **Passport Details:** 100135556. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022 **Address**: Moscow, Russian Federation. **Other Information:** Gender: male. Aleksei Morenets took

part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Aleksei Morenets was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13906.

4. **SEREBRIAKOV, Evgenii Mikhaylovich**
   DOB: 26/07/1981. **POB:** Kursk, Russian SFSR (now Russian Federation) **Nationality:** Russian **Passport Details:** 100135555. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022 **Address:** Moscow, Russian Federation. **Other Information**: Gender: male. Evgenii Serebriakov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Evgenii Serebriakov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13907.

5. **SOTNIKOV, Oleg Mikhaylovich**
   DOB: 24/08/1972. **POB:** Ulyanovsk, Russian SFSR (now Russian Federation) **Nationality:** Russian **Passport Details:** 120018866. Issued by the Ministry of Foreign Affairs of the Russian Federation. Valid from 17 April 2017 until 17 April 2022 **Address**: Moscow, Russian Federation. **Other Information**: Gender: male. Oleg Sotnikov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW), in the Netherlands. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Oleg Sotnikov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13908.

6. **ZHANG, Shilong**
   Nationality: Chinese **Address:** Hedong, Yuyang Road No 121, Tianjin, China. **Other Information:** Gender: male. Zhang Shilong is involved in “Operation Cloud Hopper”, a series of cyber-attacks. “Operation Cloud Hopper” has targeted information systems of multinational companies in six continents, including companies located in the European Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (a.k.a. “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Zhang Shilong can be linked to APT10, including through the malware he developed and tested in connection with the cyber-attacks

carried out by APT10. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating "Operation Cloud Hopper", employed Zhang Shilong. He has links with Gao Qiang, who is also designated in connection with "Operation Cloud Hopper". Zhang Shilong is therefore associated with both Huaying Haitai and Gao Qiang. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13904.

Entities

1. **CHOSUN EXPO**
   a.k.a: (1) Chosen Expo (2) Korea Export Joint Venture **Address:** DPRK. **Other Information:** Chosun Expo provided financial, technical or material support for and facilitated a series of cyberattacks, including the cyber-attacks publicly known as "WannaCry" and cyber-attacks against the Polish Financial Supervision Authority and Sony Pictures Entertainment, as well as cyber-theft from the Bangladesh Bank and attempted cyber-theft from the Vietnam Tien Phong Bank. WannaCry" disrupted information systems around the world by targeting information systems with ransomware and blocking ccess to data. It affected information systems of companies in the European Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States. The actor publicly known as "APT38" ("Advanced Persistent Threat 38") or the "Lazarus Group" carried out "WannaCry". Chosun Expo can be linked to APT38 / the Lazarus Group, including through the accounts used for the cyber-attacks. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13910.

2. **MAIN CENTRE FOR SPECIAL TECHNOLOGIES (GTSST) OF THE MAIN DIRECTORATE OF THE GENERAL STAFF OF THE ARMED FORCES OF THE RUSSIAN FEDERATION (GU/GRU)**
   Address: 22 Kirova Street, Moscow, Russian Federation. **Other Information:** The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known by its field post number 74455, is responsible for cyber-attacks, including the cyber-attacks publicly known as "NotPetya" or "EternalPetya" in June 2017 and the cyber-attacks directed at an Ukrainian power grid in the winter of 2015 and 2016. "NotPetya" or "EternalPetya" rendered data inaccessible in a number of companies in the European Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting amongst others in significant economic loss. The cyber-attack on a Ukrainian power grid resulted in parts of it being switched off during winter. The actor publicly known as "Sandworm" (a.k.a. "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" and "Telebots"), which is also behind the attack on the Ukrainian power grid, carried out "NotPetya" or "EternalPetya". The Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation has an active role in the cyber-activities undertaken by Sandworm and can be linked to Sandworm. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13911.

3. **TIANJIN HUAYING HAITAI SCIENCE AND TECHNOLOGY DEVELOPMENT CO. LTD (HUAYING HAITAI)**
   a.k.a: Haitai Technology Development Co. Ltd **Address**: Tianjin, China. **Other Information:** Huaying Haitai provided financial, technical or material support for and facilitated "Operation Cloud Hopper", a series of cyber-attacks. "Operation Cloud Hopper" has targeted information systems of multinational companies in six continents,

including companies located in the European Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (a.k.a. “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Huaying Haitai can be linked to APT10. Moreover, Huaying Haitai employed Gao Qiang and Zhang Shilong, who are both designated in connection with “Operation Cloud Hopper”. Huaying Haitai is therefore associated with Gao Qiang and Zhang Shilong. **Listed on:** 31/07/2020 **Last Updated:** 31/07/2020 **Group ID:** 13909.

Office of Financial Sanctions Implementation

HM Treasury

31/07/2020