Office of Financial
Sanctions Implementation
HM Treasury

Financial Sanctions Notice

24/11/2020

Cyber-Attacks

Introduction

1. Council Regulation (EU) 2019/796 ("the Regulation") imposing financial sanctions against Regime has been amended.

2. Identifying information for the individuals listed in the Annex to this Notice has been amended.

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

3. The following entries have been amended and are still subject to an asset freeze:

- GAO Qiang (Group ID: 13903)
- ZHANG Shilong (Group ID: 13904)

What you must do

4. 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.

5. Where a relevant institution has already reported details of accounts, other funds or economic resources held frozen for designated persons, they are not required to report these details again.

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

Legislative details

7. On 23 November 2020 Council Implementing Regulation (EU) 2020/1744 ("the Amending Regulation") was published in the Official Journal of the European Union (O.J. L 393, 23.11.2020, p.1) by the Council of the European Union.

8. The Amending Regulation amended Annex I to the Regulation with effect from 24 November 2020.

Further Information

9. 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:32020R1744&from=EN

10. 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

11. For more information please see our guide to financial sanctions:

    https://www.gov.uk/government/publications/financial-sanctions-faqs

Enquiries

12. 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

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

14. Media enquiries about the sanctions measures themselves should be addressed to the Foreign, Commonwealth & Development Office Press Office on 020 7008 3100.

ANNEX TO NOTICE

FINANCIAL SANCTIONS: CYBER-ATTACKS

COUNCIL IMPLEMENTING REGULATION (EU) 2020/1744

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

AMENDMENTS

Deleted information appears in strikethrough. Additional information appears in italics and is underlined.

Individuals

1. **GAO, Qiang**
   DOB: *04/10/1983.* **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~~ *24/11/2020* **Group ID:** 13903.

2. **ZHANG, Shilong**
   DOB: *10/09/1981.* ***POB:*** *China* **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~~ *24/11/2020* **Group ID:** 13904.

Office of Financial Sanctions Implementation

HM Treasury

24/11/2020