2026/1078

12.5.2026 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2026/1078 НА СЪВЕТА

от 11 май 2026 година

за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2019/796 на Съвета от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки ([1]), и по-специално член 13 от него,

като взе предвид предложението на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност,

като има предвид, че:

(1) На 17 май 2019 г. Съветът прие Регламент (ЕС) 2019/796.

(2) Съветът извърши преглед на списъка на физическите и юридическите лица, образуванията и органите, съдържащ се в приложение I към Регламент (ЕС) 2019/796. Въз основа на този преглед следва да бъдат актуализирани основанията за включването на четири лица и едно образувание в списъка на физическите и юридическите лица, образуванията и органите, по отношение на които се прилагат ограничителни мерки.

(3) Поради това приложение I към Регламент (ЕС) 2019/796 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Приложение I към Регламент (ЕС) 2019/796 се изменя в съответствие с приложението към настоящия регламент.

Член 2

Настоящият регламент влиза в сила в деня след публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 11 май 2026 година.

За Съвета

Председател

K. KALLAS

([1]) ОВ L 129 I, 17.5.2019 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ПРИЛОЖЕНИЕ

Приложение I към Регламент (ЕС) 2019/796 се изменя, както следва:

1) В раздел „A. Физически лица“ вписвания 1, 2, 13 и 14 се заменят със следните съответни вписвания:

	Име	Идентификационни данни	Основания	Дата на вписване
„1.	GAO Qiang	Дата на раждане: 4 октомври 1983 г. Място на раждане: Shandong Province, Китай Адрес: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Китай Гражданство: китайско Пол: мъжки	Gao Qiang е свързан с групировката чадър APT10 („Advanced Persistent Threat 10“) (изв. още като „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium“) и е участвал в „Операция Cloud Hopper“ – серия кибератаки със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави. Мишена на „Операция Cloud Hopper“ са били информационните системи на многонационални дружества на шест континента, включително дружества в Съюза, при което е осъществен неразрешен достъп до чувствителни търговски данни, довел до значителни икономически загуби. Gao Qiang е свързан с командната и контролната инфраструктура на APT10. Освен това Gao Qiang е работил за Huaying Haitai — дружество, използвано от APT10 и посочено като оказало подкрепа и създавало улеснения за „Операция Cloud Hopper“. Той е свързан и с Zhang Shilong, който е свързан с APT10 и който също е работил за Huaying Haitai.	30.7.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
2.	ZHANG Shilong	Дата на раждане: 10 септември 1981 г. Място на раждане: Китай Адрес: Hedong, Yuyang Road № 121, Tianjin, Китай Гражданство: китайско Пол: мъжки	Zhang Shilong е свързан с групировката чадър APT10 („Advanced Persistent Threat 10“) (изв. още като „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium“) и е участвал в „Операция Cloud Hopper“ – серия кибератаки със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави. Мишена на „Операция Cloud Hopper“ са информационните системи на многонационални дружества на шест континента, включително дружества в Съюза, при което е осъществен неразрешен достъп до чувствителни търговски данни, довел до значителни икономически загуби. Zhang Shilong е свързан с APT10, включително чрез зловредния софтуер, разработен и тестван от него във връзка с извършените от APT10 кибератаки. Освен това Zhang Shilong е работил за Huaying Haitai — дружество, използвано от APT10 и посочено като оказало подкрепа и създавало улеснения за „Операция Cloud Hopper“. Той е свързан с Gao Qiang, който от своя страна е свързан с APT10 и който е работил за Huaying Haitai.	30.7.2020 г.

	Име	Идентификационни данни	Основания	Дата на вписване
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Дата на раждане: 20.4.1989 г. Място на раждане: Serpukhov, Руска федерация Гражданство: руско Адрес: Serpukhov Пол: мъжки	Mikhail Mikhailovich Tsarev е участвал в кибератаки със значително въздействие, които представляват външна заплаха за държавите – членки на ЕС. Mikhail Mikhailovich Tsarev, известен и с онлайн псевдонимите Mango, Alexander Grachev, Super Misha, Ivanov Mixail, Misha Krutysha и Nikita Andreevich Tsarev, е ключов участник при внедряването на зловредните софтуерни програми Conti и Trickbot и е участник в базираната в Русия група за заплахи Wizard Spider. Wizard Spider продължава да развива и засилва дейността си. Зловредните софтуерни програми Conti и Trickbot бяха създадени и разработени от Wizard Spider. Wizard Spider е провел кампании със софтуер за изнудване в различни сектори, включително основни услуги като здравеопазването и банковото дело. Групата е заразила компютри в световен мащаб и нейният зловреден софтуер е разработен в силно модулен зловреден софтуерен пакет. Кампаниите на Wizard Spider с използване на зловреден софтуер като Conti, Ryuk, TrickBot или Black Basta са причина за значителни икономически щети в Европейския съюз. Следователно Mikhail Mikhailovich Tsarev участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.	24.6.2024 г.

ELI: http://data.europa.eu/eli/reg_impl/2026/1078/oj

	Име	Идентификационни данни	Основания	Дата на вписване
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Дата на раждане: 19.5.1982 г. Място на раждане: Abakan, Руска федерация Гражданство: руско Пол: мъжки	Maksim Galochkin е участвал в кибератаки със значително въздействие, които представляват външна заплаха за държавите – членки на ЕС. Maksim Galochkin е известен и с онлайн псевдонимите Benalen, Bentley, Volhvb, volhvb, manuel, Max17 и Crypt. Galochkin е ключов участник при внедряването на зловредните софтуерни програми TrickBot и Conti и е участник в базираната в Русия група за заплахи Wizard Spider. Ръководи група от лица, провеждащи тестове, с отговорности за разработването, надзора и провеждането на тестове на зловредната програма TrickBot, създадена и внедрена от Wizard Spider. Wizard Spider продължава да развива и засилва дейността си. Wizard Spider провежда кампании със софтуер за изнудване в различни сектори, включително основни услуги като здравеопазването и банковото дело. Групата е заразила компютри в световен мащаб и нейният зловреден софтуер е разработен в силно модулен зловреден софтуерен пакет. Кампаниите на Wizard Spider с използване на зловреден софтуер като Conti, Ryuk, TrickBot или Black Basta са причина за значителни икономически щети в Европейския съюз. Следователно Maksim Galochkin участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.	24.6.2024 г.“

2) В раздел „Б. Юридически лица, образувания и органи“ вписване 1 се заменя със следното:

	Наименование	Идентификационни данни	Основания	Дата на вписване
„1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Известно също като: Haitai Technology Development Co. Ltd Местоположение: Tianjin, Китай	Huaying Haitai е предоставил финансова, техническа или материална подкрепа и е улеснявал „Операция Cloud Hopper“ – серия кибератаки със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави. Мишена на „Операция Cloud Hopper“ са информационните системи на многонационални дружества на шест континента, включително дружества на територията на Съюза, при което е осъществен неразрешен достъп до чувствителни търговски данни, довел до значителни икономически загуби. „Операция Cloud Hopper“ е дело на извършител, известен в публичното пространство като „APT10“ („Advanced Persistent Threat 10“) (изв. още като „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium“). Huaying Haitai може да бъде свързано с APT10. Освен това за Huaying Haitai работят Gao Qiang и Zhang Shilong, които са посочени като свързани с „Операция Cloud Hopper“. Следователно Huaying Haitai също е свързано с Gao Qiang и Zhang Shilong.	30.7.2020 г.“