2024/1778

24.6.2024 г.

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2024/1778 НА СЪВЕТА

от 24 юни 2024 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, параграф 1 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) Целенасочените ограничителни мерки срещу кибератаки със значително въздействие, представляващи външна заплаха за Съюза или неговите държави членки, са една от мерките, включени в рамката на Съюза за съвместен дипломатически отговор на злонамерени действия в киберпространството („инструментариум за кибердипломация“), и са жизненоважен инструмент за предотвратяването, възпирането, разколебаването и реагирането на такива действия.

(3) Увеличават се броят, честотата и сложността на злонамерените действия в киберпространството срещу критична инфраструктура или основни услуги, включително чрез използването на софтуер за изнудване и за заличаване на съдържание (wiper), прицелването във веригите на доставки и кибершпионажът, включително дейностите по кражба на интелектуална собственост. Поради смущенията и разрушителните последици от тези дейности, те представляват системна заплаха за сигурността, икономиката, демокрацията и обществото като цяло в Съюза.

(4) Използването на кибероперации, които подпомогнаха и съпътстваха непредизвиканата и неоправдана агресивна война на Русия срещу Украйна, засяга глобалната стабилност и сигурност, представлява значителен риск от ескалация и допринася за вече значителния ръст на злонамерените действия в киберпространството извън контекста на въоръжен конфликт през последните години. Нарастващите рискове за киберсигурността и цялостната сложна картина на киберзаплахите, с очевиден риск от бързо разпространение на киберинциденти от една държава членка към други и от трети държави към Съюза, допълнително налагат ограничителни мерки съгласно Регламент (ЕС) 2019/796.

(5) Като част от непрекъснатите, целенасочени и координирани действия на Съюза срещу настойчивите участници в киберзаплахи, в списъка на подлежащите на ограничителни мерки физически и юридически лица, образувания и органи, съдържащ се в приложение I към Регламент (ЕС) 2019/796, следва да бъдат включени шест физически лица. Тези лица са отговорни или са участвали в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.

(6) 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 съгласно приложението към настоящия регламент.

([1]) ОВ L 129 I, 17.5.2019 г., стр. 1.

Член 2

Настоящият регламент влиза в сила в деня на 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 Люксембург на 24 юни 2024 година.

За Съвета

Председател

J. BORRELL FONTELLES

ПРИЛОЖЕНИЕ

В раздел „А. Физически лица“ в приложение I към Регламент (ЕС) 2019/796 се добавят следните вписвания:

	Име	Идентификационни данни	Основания	Дата на вписване
„9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Дата на раждане: 3.8.1985 г. Гражданство: руско Пол: мъжки	Ruslan PERETYATKO е участвал в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки. Ruslan PERETYATKO е част от групата „Callisto“ (Callisto group) на офицери от руското военно разузнаване, които провеждат кибероперации срещу държави — членки на ЕС, и трети държави. Callisto Group (известна също като Seaborgium, Star Blizzard, ColdRiver, TA446) стартира многогодишни фишинг кампании, използвани за кражба на идентификационна информация и данни от профили. Освен това Callisto Group е отговорна за кампании, насочени към отделни лица и критични държавни функции, включително в областта на отбраната и външните отношения. Ето защо Ruslan PERETYATKO участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.	24.6.2024 г.
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Дата на раждане: 18.5.1987 г. Място на раждане: град Сиктивкар, Русия Гражданство: руско Пол: мъжки	Andrey Stanislavovich KORINETS е участвал в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки. Andrey Stanislavovich KORINETS е офицер на „Център 18“ (Center 18) на Федералната служба за сигурност на Руската федерация. Andrey Stanislavovich KORINETS е част от Callisto Group на офицери от руското военно разузнаване, които провеждат кибероперации срещу държави — членки на ЕС, и трети държави. Callisto Group (известна също като Seaborgium, Star Blizzard, ColdRiver, TA446) стартира многогодишни фишинг кампании, използвани за кражба на идентификационна информация и данни от профили. Освен това Callisto Group е отговорна за кампании, насочени към отделни лица и критични държавни функции, включително в областта на отбраната и външните отношения. Ето защо Andrey Stanislavovich KORINETS участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.	24.6.2024 г.

	Име	Идентификационни данни	Основания	Дата на вписване
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (изписване на руски език) Олександр СКЛЯНКО (изписване на украински език) Дата на раждане: 5.8.1973 г. Паспорт: ЕС 867868, издаден на 27.11.1998 г. (Украйна) Пол: мъжки	Oleksandr SKLIANKO е участвал в кибератаки със значително въздействие срещу държави — членки на ЕС, както и в кибератаки със значително въздействие срещу трети държави. Oleksandr SKLIANKO е част от хакерската група Armageddon, подкрепена от Федералната служба за сигурност на Руската федерация, която е извършила различни кибератаки със значително въздействие срещу правителството на Украйна и държавите — членки на ЕС, и техни правителствени служители, включително чрез фишинг имейли и кампании със зловреден софтуер. Ето защо Oleksandr SKLIANKO участва в кибератаки със значително въздействие срещу трети държави, както и в кибератаки, които представляват външна заплаха за Съюза или неговите държави членки.	24.6.2024 г.
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (изписване на руски език) Микола ЧЕРНИХ (изписване на украински език) Дата на раждане: 12.10.1978 г. Паспорт: ЕС 922162, издаден на 20.1.1999 г. (Украйна) Пол: мъжки	Mykola CHERNYKH е участвал в кибератаки със значително въздействие срещу държави — членки на ЕС, както и в кибератаки със значително въздействие срещу трети държави. Mykola CHERNYKH е част от хакерската група Armageddon, подкрепена от Федералната служба за сигурност на Руската федерация, която е извършила различни кибератаки със значително въздействие срещу правителството на Украйна и държавите — членки на ЕС, и техни правителствени служители, включително чрез фишинг имейли и кампании със зловреден софтуер. В качеството си на бивш служител на Службата за сигурност на Украйна той е обвинен в държавна измяна и незаконна намеса в работата на електронни изчислителни машини и автоматизирани системи. Ето защо Mykola CHERNYKH участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.	24.6.2024 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: Серпухов, Руска федерация Гражданство: руско Адрес: Серпухов 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 . Зловредните софтуерни програми Conti и Trickbot бяха създадени и разработени от Wizard Spider. 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 техният зловреден софтуер е разработен в силно модулен зловреден софтуерен пакет. Кампаниите на Wizard Spider с използване на зловреден софтуер като Conti, Ryuk и TrickBot, са причина за значителни икономически щети в Европейския съюз. Ето защо Mikhail Mikhailovich TSAREV участва в кибератаки със значително въздействие, които представляват външна заплаха за Съюза или неговите държави членки.	24.6.2024 г.

	Име	Идентификационни данни	Основания	Дата на вписване
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Дата на раждане: 19.5.1982 г. Място на раждане: Абакан, 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 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 техният зловреден софтуер е разработен в силно модулен зловреден софтуерен пакет. Кампаниите на Wizard Spider с използване на зловреден софтуер като Conti, Ryuk и TrickBot, са причина за значителни икономически щети в Европейския съюз. Ето защо Maksim Galochkin 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/2024/1778/oj