2024/1391

17.5.2024

DECIZIA (PESC) 2024/1391 A CONSILIULUI

din 17 mai 2024

de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 29,

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 17 mai 2019, Consiliul a adoptat Decizia (PESC) 2019/797 ([1]).

(2) Decizia (PESC) 2019/797 se aplică până la 18 mai 2025. Pe baza reexaminării deciziei menționate, valabilitatea măsurilor restrictive prevăzute în aceasta ar trebui să fie prelungită până la data respectivă.

(3) Având în vedere continuarea și intensificarea comportamentului ostil în spațiul cibernetic, inclusiv a comportamentului îndreptat împotriva unor state terțe, ar trebui să fie actualizate motivele includerii a șase persoane și a două entități pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsuri restrictive prevăzută în anexa la Decizia (PESC) 2019/797.

(4) Prin urmare, Decizia (PESC) 2019/797 ar trebui să fie modificată în consecință,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Decizia (PESC) 2019/797 se modifică după cum urmează:

1. Articolul 10 se înlocuiește cu următorul text:

   „*Articolul 10*

   Prezenta decizie se aplică până la 18 mai 2025 și se reexaminează permanent.”

2. Anexa se modifică în conformitate cu anexa la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 17 mai 2024.

Pentru Consiliu

Președintele

H. LAHBIB

([1]) Decizia (PESC) 2019/797 a Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 129 I, 17.5.2019, p. 13).

ANEXĂ

Anexa la Decizia (PESC) 2019/797 („Lista persoanelor fizice și juridice, a entităților și a organismelor menționate la articolele 4 și 5”) se modifică după cum urmează:

1. La secțiunea „A. Persoane fizice”, rubricile 3-8 se înlocuiesc cu următorul text:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data nașterii: 27.5.1972 Locul nașterii: Regiunea Perm, RSFS Rusă (în prezent Federația Rusă) Numărul pașaportului: 120017582 Eliberat de: Ministrul de Externe al Federației Ruse valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenia: rusă Sexul: masculin	Alexey Minin a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer de sprijin specializat în informații din surse umane al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), Alexey Minin a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină acces neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua WiFi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Alexey Minin, ca ofițer al Direcției principale de informații a Rusiei (GRU), pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data nașterii: 31.7.1977 Locul nașterii: Regiunea Murmansk, RSFS Rusă (în prezent Federația Rusă) Numărul pașaportului: 100135556 Eliberat de: Ministrul de Externe al Federației Ruse valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenia: rusă Sexul: masculin	Alexey Morenets a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de operator informatic pentru Direcția principală a Statului--Major al forțelor armate ruse (GU/GRU), Aleksei Morenets a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină acces neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua WiFi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen-en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Alexey Morenets ca membru al unității militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data nașterii: 26.7.1981 Locul nașterii: Kursk, RSFS Rusă (în prezent, Federația Rusă) Numărul pașaportului: 100135555 Eliberat de: Ministrul de Externe al Federației Ruse valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenia: rusă Sexul: masculin	Evgenii Serebriakov a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de operator informatic pentru Direcția principală a Statului--Major al forțelor armate ruse (GU/GRU), Evgenii Serebriakov a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină acces neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua WiFi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen-en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Din primăvara anului 2022, Evgenii Serebriakov conduce «Sandworm» (*alias* «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» și «Telebots»), un actor și un grup de piraterie informatică afiliat unității 74455 a Direcției principale de informații ruse. Sandworm a desfășurat atacuri cibernetice asupra Ucrainei, inclusiv asupra agențiilor guvernamentale ucrainene, în urma războiului de agresiune al Rusiei împotriva Ucrainei.	30.7.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj

	Nume	Informații de identificare	Motive	Data includerii pe listă
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data nașterii: 24.8.1972 Locul nașterii: Ulianovsk, RSFS Rusă (în prezent, Federația Rusă) Numărul pașaportului: 120018866 Eliberat de: Ministrul de Externe al Federației Ruse valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenia: rusă Sexul: masculin	Oleg Sotnikov a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer de sprijin specializat în informații din surse umane al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), Oleg Sotnikov a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină acces neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua WiFi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest l-a pus sub acuzare pe Oleg Sotnikov ca ofițer al Direcției principale de informații a Rusiei (GRU), pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
7.	Dmitri Sergheevici BADIN	Дмитрий Сергеевич БАДИН Data nașterii: 15.11.1990 Locul nașterii: Kursk, RSFS Rusă (în prezent, Federația Rusă) Cetățenia: rusă Sexul: masculin	Dmitri Badin a luat parte la un atac cibernetic cu efecte importante împotriva parlamentului federal german (Deutscher Bundestag) și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer în serviciul militar de informații al celui de al 85-lea Centru principal de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU), Dmitri Badin a făcut parte dintr-o echipă de ofițeri ai serviciului militar de informații rus care a organizat un atac cibernetic împotriva parlamentului federal german în aprilie și mai 2015. Respectivul atac cibernetic a fost îndreptat împotriva sistemului informatic al parlamentului, căruia i-a afectat funcționarea timp de mai multe zile. A fost furat un volum important de date și au fost afectate conturile de e-mail ale mai multor parlamentari, precum și cel al fostului cancelar Angela Merkel. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Dmitry Badin ca membru al unității militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	22.10.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj

	Nume	Informații de identificare	Motive	Data includerii pe listă
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data nașterii: 21.2.1961 Cetățenia: rusă Sexul: masculin	Igor Kostyukov este actualul șef al Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU), unde a ocupat anterior funcția de prim-șef adjunct. Una dintre unitățile aflate sub comanda sa este cel de al 85-lea Centru principal de servicii speciale (GTsSS) (*alias* «unitatea militară 26165», «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» și «Strontium»). În această calitate, Igor Kostyukov este responsabil de atacurile cibernetice desfășurate de GTsSS, inclusiv de atacuri cu efecte importante care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre. În special, ofițerii serviciului militar de informații al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) din aprilie și mai 2015, precum și la tentativa de atac cibernetic din aprilie 2018 care a avut drept scop piratarea rețelei Wi-fi a Organizației pentru Interzicerea Armelor Chimice (OIAC) din Țările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, căruia i-a afectat funcționarea timp de mai multe zile. A fost furat un volum important de date și au fost afectate conturile de e-mail ale mai multor parlamentari, precum și cel al fostului cancelar Angela Merkel.	22.10.2020”.

2. La secțiunea „B. Persoane juridice, entități și organisme”, rubricile 3 și 4 se înlocuiesc cu următorul text:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [Centrul principal pentru tehnologii speciale (GTsST) al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU)]	Adresă: 22 Kirova Street, Moscow, Russian Federation (str. Kirova nr. 22, Moscova, Federația Rusă)	Centrul principal pentru tehnologii speciale (GTsST) al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), cunoscut și prin codul său poștal de teren 74455, este implicat într-o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe, inclusiv atacurile cibernetice cunoscute în mod public sub numele «NotPetya» sau «EternalPetya» din iunie 2017 și atacurile cibernetice îndreptate împotriva unui sistem electroenergetic ucrainean din iarna anilor 2015 și 2016. «NotPetya» sau «EternalPetya» a blocat accesul la date în mai multe întreprinderi din Uniune, din Europa în ansamblu și din întreaga lume, prin vizarea computerelor prin programe de tip ransomware și prin blocarea accesului la date, ceea ce a dus, printre altele, la pierderi economice importante. Atacul cibernetic asupra unui sistem electroenergetic ucrainean a condus la întreruperea unor porțiuni ale acestuia în timpul iernii. Actorul cunoscut în mod public sub numele de «Sandworm» (*alias* «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» și «Telebots»), aflat, de asemenea, în spatele atacului asupra sistemului electroenergetic ucrainean, a comis atacul «NotPetya» sau «EternalPetya». Sandworm a desfășurat atacuri cibernetice împotriva Ucrainei, inclusiv asupra agențiilor guvernamentale ucrainene și asupra infrastructurii critice ucrainene, în urma războiului de agresiune al Rusiei împotriva Ucrainei. Printre respectivele atacuri cibernetice se numără campanii de spear-phishing, atacuri de tip malware și ransomware. Centrul principal pentru tehnologii speciale al Direcției principale a Statului-Major al forțelor armate ruse din Federația Rusă are un rol activ în activitățile cibernetice desfășurate de Sandworm și poate fi stabilită o legătură între centru și acesta.	30.7.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj

	Nume	Informații de identificare	Motive	Data includerii pe listă
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [Cel de al 85-lea Centru principal de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU)]	Adresă: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation (Komsomol'ski Prospekt, 20, Moscova, 119146, Federația Rusă)	Cel de al 85-lea Centru principal de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU) (*alias* «unitatea militară 26165», «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» și «Strontium») este implicat în atacuri cibernetice cu efecte semnificative care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre și în atacuri cibernetice cu efecte semnificative împotriva unor state terțe. În special, ofițerii serviciului militar de informații al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) în aprilie și mai 2015, precum și la tentativa de atac cibernetic din aprilie 2018 care a avut drept scop piratarea rețelei Wi-fi a Organizației pentru Interzicerea Armelor Chimice (OIAC) din Țările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, căruia i-a afectat funcționarea timp de mai multe zile. A fost furat un volum important de date și au fost afectate conturile de e-mail ale mai multor parlamentari, precum și cel al fostului cancelar Angela Merkel. În urma războiului de agresiune al Rusiei împotriva Ucrainei, au fost comise atacuri cibernetice împotriva Ucrainei de către GTsSS (atacuri de tip spear-phishing și atacuri malware).	22.10.2020".