2024/1778

24.6.2024

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2024/1778 AL CONSILIULUI

din 24 iunie 2024

privind punerea în aplicare a Regulamentului (UE) 2019/796 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 funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre ([1]), în special articolul 13 alineatul (1),

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

întrucât:

(1) La 17 mai 2019, Consiliul a adoptat Regulamentul (UE) 2019/796.

(2) Măsurile restrictive specifice împotriva atacurilor cibernetice având efecte importante care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre sunt una dintre măsurile incluse în cadrul Uniunii privind un răspuns diplomatic comun la activitățile cibernetice răuvoitoare (Setul de instrumente pentru diplomația cibernetică), precum și un instrument vital pentru a preveni, a împiedica și a descuraja atacurile cibernetice și a răspunde la acestea.

(3) Activitățile cibernetice răuvoitoare împotriva infrastructurii critice sau a serviciilor esențiale, inclusiv prin utilizarea atacurilor de tip ransomware și a celor care vizează ștergerea datelor (*wiper*), atacarea lanțurilor de aprovizionare și spionajul cibernetic, inclusiv activitățile de furt de proprietate intelectuală, sunt în creștere ca număr, frecvență și complexitate. Având în vedere efectele lor perturbatoare și distructive, aceste activități reprezintă o amenințare sistemică la adresa securității, a economiei, a democrației Uniunii și a societății în general.

(4) Recurgerea la operațiuni cibernetice care au înlesnit și au însoțit războiul de agresiune neprovocat și nejustificat al Rusiei împotriva Ucrainei afectează stabilitatea și securitatea mondială, reprezintă un risc important de escaladare și se adaugă creșterii deja semnificative, în ultimii ani, a activităților cibernetice răuvoitoare în afara contextului conflictelor armate. Riscurile tot mai mari în materie de securitate cibernetică și un peisaj general complex al amenințărilor cibernetice, cu un risc clar de propagare rapidă a incidentelor cibernetice de la un stat membru la altul și din țări terțe către Uniune, impun, de asemenea, măsuri restrictive în temeiul Regulamentului (UE) 2019/796.

(5) Ca parte a acțiunii susținute, adaptate și coordonate a Uniunii împotriva entităților care reprezintă amenințări cibernetice persistente, șase persoane fizice ar trebui să fie incluse pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsurile restrictive prevăzută în anexa I la Regulamentul (UE) 2019/796. Persoanele respective sunt responsabile pentru atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre sau au fost implicate în astfel de atacuri.

(6) Prin urmare, anexa I la Regulamentul (UE) 2019/796 ar trebui să fie modificată în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Anexa I la Regulamentul (UE) 2019/796 se modifică în conformitate cu anexa la prezentul regulament.

([1]) JO L 129 I, 17.5.2019, p. 1.

Articolul 2

Prezentul regulament intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Luxemburg, 24 iunie 2024.

Pentru Consiliu

Președintele

J. BORRELL FONTELLES

ANEXĂ

La secțiunea „A. Persoane fizice” din anexa I la Regulamentul (UE) 2019/796 se adaugă următoarele rubrici:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Data nașterii: 3.8.1985 Cetățenia: rusă Sexul: masculin	Ruslan Peretyatko a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre. Ruslan Peretyatko face parte din «grupul Callisto» format din ofițeri de informații militari ruși care desfășoară operațiuni cibernetice împotriva statelor membre ale UE și împotriva unor state terțe. Grupul Callisto (cunoscut și sub denumirea de «Seaborgium», «Star Blizzard», «ColdRiver», «TA446») a lansat campanii multianuale de phishing utilizate pentru a fura date din conturi și elementele personale de acces la acestea. În plus, grupul Callisto este responsabil de campanii care vizează persoane și funcții critice ale statului, inclusiv în domeniul apărării și al relațiilor externe. Prin urmare, Ruslan Peretyatko este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Data nașterii: 18.5.1987 Locul nașterii: orașul Syktyvkar, Rusia Cetățenia: rusă Sexul: masculin	Andrey Stanislavovich Korinets a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre. Andrey Stanislavovich Korinets este ofițer al «Centrului 18» al Serviciului Federal de Securitate (FSB) al Federației Ruse. Andrey Stanislavovich Korinets face parte din «grupul Callisto» format din ofițeri de informații militari ruși care desfășoară operațiuni cibernetice împotriva statelor membre ale UE și împotriva unor state terțe. Grupul Callisto (cunoscut și sub denumirea de «Seaborgium», «Star Blizzard», «ColdRiver», «TA446») a lansat campanii multianuale de phishing utilizate pentru a fura date din conturi și elementele personale de acces la acestea. În plus, grupul Callisto este responsabil de campanii care vizează persoane și funcții critice ale statului, inclusiv în domeniul apărării și al relațiilor externe. Prin urmare, Andrey Stanislavovich Korinets este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024

	Nume	Informații de identificare	Motive	Data includerii pe listă
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (ortografie rusă) Олександр СКЛЯНКО (ortografie ucraineană) Data naşterii: 5.8.1973 Paşaport: EC 867868, eliberat la 27.11.1998 (Ucraina) Sexul: masculin	Oleksandr Sklianko a participat la atacuri cibernetice cu un efect semnificativ împotriva statelor membre ale UE, precum și la atacuri cibernetice cu un efect semnificativ împotriva unor state terțe. Oleksandr Sklianko face parte din grupul de hackeri Armageddon sprijinit de Serviciul Federal de Securitate (FSB) al Federației Ruse, care a desfășurat diverse atacuri cibernetice cu un efect semnificativ asupra guvernului Ucrainei și asupra statelor membre ale UE și a funcționarilor lor guvernamentali, inclusiv prin utilizarea de e-mailuri de phishing și campanii de malware. Prin urmare, Oleksandr Sklianko este implicat în atacuri cibernetice cu un efect semnificativ împotriva unor state terțe, precum și în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (ortografie rusă) Микола ЧЕРНИХ (ortografie ucraineană) Data naşterii: 12.10.1978 Paşaport: CE 922162, eliberat la 20.1.1999 (Ucraina) Sexul: masculin	Mykola Chernykh a participat la atacuri cibernetice cu un efect semnificativ împotriva statelor membre ale UE, precum și la atacuri cibernetice cu un efect semnificativ împotriva unor state terțe. Mykola Chernykh face parte din grupul de hackeri Armageddon sprijinit de Serviciul Federal de Securitate (FSB) al Federației Ruse, care a desfășurat diverse atacuri cibernetice cu un efect semnificativ asupra guvernului Ucrainei și asupra statelor membre ale UE și a funcționarilor lor guvernamentali, inclusiv prin utilizarea e-mailurilor de phishing și a campaniilor de malware. În calitate de fost angajat al Serviciului de Securitate al Ucrainei, este acuzat în Ucraina de trădare și intervenție neautorizată în funcționarea mașinilor electronice de calcul și a sistemelor automatizate. Prin urmare, Mykola Chernykh este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024

	Nume	Informații de identificare	Motive	Data includerii pe listă
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data nașterii: 20.4.1989 Locul nașterii: Serpukhov, Federația Rusă Cetățenia: rusă Adresă: Serpukhov Sexul: masculin	Mikhail Mikhailovich Tsarev a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale UE. Mikhail Mikhailovich Tsarev, cunoscut și sub pseudonimele online «Mango», «Alexander Grachev», «Super Misha», «Ivanov Mixail», «Misha Krutysha» și «Nikita Andreevich Tsarev», este un actor-cheie în răspândirea programelor de malware «Conti» și «Trickbot» și este implicat în grupul ostil «Wizard Spider» din Rusia. Programele de malware «Conti» și «Trickbot» au fost create și dezvoltate de Wizard Spider. Wizard Spider a desfășurat campanii de tip ransomware în diverse sectoare, inclusiv servicii esențiale cum ar fi sănătatea și serviciile bancare. Grupul a infectat computere în întreaga lume, iar programele sale malware au fost dezvoltate într-un ansamblu de programe malware foarte modular. Campaniile desfășurate de Wizard Spider, prin utilizarea de programe de malware cum ar fi Conti, «Ryuk» și TrickBot, sunt responsabile pentru daune economice substanțiale în Uniunea Europeană. Prin urmare, Mikhail Mikhailovich Tsarev este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024

	Nume	Informații de identificare	Motive	Data includerii pe listă
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data nașterii: 19.5.1982 Locul nașterii: Abakan, Federația Rusă Cetățenia: rusă Sexul: masculin	Maksim Galochkin a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale UE. Maksim Galochkin cunoscut și sub pseudonimele online «Benalen», «Bentley», «Volhvb», «volhvb», «manuel», «Max17» și «Crypt». Galochkin este un actor-cheie în răspândirea programelor de malware «Conti» și «Trickbot» și este implicat în grupul ostil «Wizard Spider» din Rusia. Acesta a condus un grup de testeri cu responsabilități în dezvoltarea, controlul și aplicarea testelor pentru programul de spionare TrickBot, creat și desfășurat de Wizard Spider. Wizard Spider a desfășurat campanii de tip ransomware în diverse sectoare, inclusiv servicii esențiale cum ar fi sănătatea și serviciile bancare. Grupul a infectat computere în întreaga lume, iar programele sale malware au fost dezvoltate într-un ansamblu de programe malware foarte modular. Campaniile desfășurate de Wizard Spider, prin utilizarea de programe de malware cum ar fi Conti, «Ryuk» și TrickBot, sunt responsabile pentru daune economice substanțiale în Uniunea Europeană. Prin urmare, Maksim Galochkin este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024”