2024/1778

24.6.2024

RÅDETS GENOMFÖRANDEFÖRORDNING (EU) 2024/1778

av den 24 juni 2024

om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av rådets förordning (EU) 2019/796 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater [1], särskilt artikel 13.1,

med beaktande av förslaget från unionens höga representant för utrikes frågor och säkerhetspolitik, och

av följande skäl:

(1) Den 17 maj 2019 antog rådet förordning (EU) 2019/796.

(2) Riktade restriktiva åtgärder mot cyberattacker med en betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater, är en av de åtgärder som ingår i unionens ram för en gemensam diplomatisk respons mot skadlig it-verksamhet (verktygslådan för cyberdiplomati) och ett viktigt instrument för att förebygga, motverka, avskräcka, och bemöta sådan verksamhet.

(3) Skadlig it-verksamhet mot kritisk infrastruktur eller grundläggande tjänster, bland annat genom användning av utpressningsprogram och wipers, inriktning på leveranskedjor och it-spionage, inbegripet stöld av immateriella rättigheter, blir allt vanligare, mer frekvent och sofistikerad. Med sina omvälvande och destruktiva effekter utgör sådan verksamhet ett systemhot mot unionens säkerhet, ekonomi, demokrati och samhället i stort.

(4) Användning av cyberinsatser har möjliggjort och åtföljt Rysslands oprovocerade och oberättigade anfallskrig mot Ukraina, vilket påverkar den globala stabiliteten och säkerheten, utgör en betydande risk för upptrappning och bidrar till den redan betydande ökningen av skadlig it-verksamhet utanför väpnade konflikter under de senaste åren. De växande cybersäkerhetsriskerna och den övergripande komplexa cyberhotbilden, med en tydlig risk för snabba spridningseffekter av cyberincidenter från en medlemsstat till andra och från tredjeländer till unionen, kräver ytterligare restriktiva åtgärder enligt förordning (EU) 2019/796.

(5) Som en del i de kontinuerliga, skräddarsydda och samordnade unionsinsatserna mot aktörer som utgör ett ihållande cyberhot bör sex fysiska personer föras upp på förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för restriktiva åtgärder som anges i bilaga I till förordning (EU) 2019/796. Dessa personer är ansvariga för eller har varit inblandade i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.

(6) Bilaga I till förordning (EU) 2019/796 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Bilaga I till förordning (EU) 2019/796 ska ändras i enlighet med bilagan till den här förordningen.

[1] EUT L 129 I, 17.5.2019, s. 1.

Artikel 2

Denna förordning träder i kraft samma dag som det offentliggörs i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Luxemburg den 24 juni 2024.

På rådets vägnar

J. BORRELL FONTELLES

Ordförande

BILAGA

Följande poster ska läggas till i avsnitt ”A. Fysiska personer” i bilaga I till förordning (EU) 2019/796:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Födelsedatum: 3.8.1985 Nationalitet: rysk Kön: man	Ruslan PERETYATKO var inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater. Ruslan PERETYATKO ingår i ’Callisto-gruppen’, som består av ryska militära underrättelseofficerare som utför cyberoperationer mot EU-medlemsstater och tredjeländer. Callisto Group (även kallad ’Seaborgium’, ’Star Blizzard’, ’ColdRiver’, ’TA446’) har inlett fleråriga nätfiskekampanjer som används för att stjäla kontouppgifter och kontodata. Callisto-gruppen är dessutom ansvarig för kampanjer riktade mot enskilda personer och kritiska statliga funktioner, bland annat på områdena försvar och yttre förbindelser. Ruslan PERETYATKO är därför inblandad i cyberattacker med en betydande effekt, som utgör ett externt hot mot unionen eller dess medlemsstater.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Födelsedatum: 18.5.1987 Födelseort: Staden Syktyvkar, Ryssland Nationalitet: rysk Kön: man	Andrey Stanislavovich KORINETS var inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater. Andrey Stanislavovich KORINETS är officer i ’Center 18’ vid Ryska federationens federala säkerhetstjänst (FSB). Andrey Stanislavovich KORINETS ingår i ’Callisto-gruppen’, som består av ryska militära underrättelseofficerare som utför cyberoperationer mot EU-medlemsstater och tredjeländer. Callisto Group (även kallad ’Seaborgium’, ’Star Blizzard’, ’ColdRiver’, ’TA446’) har inlett fleråriga nätfiskekampanjer som används för att stjäla kontouppgifter och kontodata. Callisto-gruppen är dessutom ansvarig för kampanjer riktade mot enskilda personer och kritiska statliga funktioner, bland annat på områdena försvar och yttre förbindelser. Andrey Stanislavovich KORINETS är därför inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.	24.6.2024

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (rysk stavning) Олександр СКЛЯНКО (ukrainsk stavning) Födelsedatum: 5.8.1973 Passnummer: EC 867868, utfärdat den 27.11.1998 (Ukraina) Kön: man	Oleksandr SKLIANKO var inblandad i cyberattacker med betydande effekter mot EU:s medlemsstater samt cyberattacker med betydande inverkan på tredjeländer. Oleksandr SKLIANKO ingår i hackergruppen Armageddon som stöds av Ryska federationens federala säkerhetstjänst (FSB) och som genomförde olika cyberattacker med betydande inverkan på Ukrainas regering och på EU:s medlemsstater och deras regeringstjänstemän, bland annat genom att använda e-post för nätfiske och kampanjer med skadlig programvara. Oleksandr SKLIANKO är därför inblandad i cyberattacker med en betydande effekt mot tredjestater samt i cyberattacker med en betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (rysk stavning) Микола ЧЕРНИХ (ukrainsk stavning) Födelsedatum: 12.10.1978 Passnummer: EC 922162, utfärdat den 20.1.1999 (Ukraina) Kön: man	Mykola CHERNYKH var inblandad i cyberattacker med betydande effekter mot EU:s medlemsstater samt cyberattacker med betydande inverkan på tredjeländer. Mykola CHERNYKH ingår i hackergruppen Armageddon som stöds av Ryska federationens FSB och som genomförde olika cyberattacker med betydande inverkan på Ukrainas regering och på EU:s medlemsstater och deras regeringstjänstemän, bland annat genom att använda e-post för nätfiske och kampanjer med skadlig programvara. Som tidigare anställd vid Ukrainas säkerhetstjänst står han åtalad i Ukraina för förräderi och obehörigt intrång i driften av elektroniska datormaskiner och automatiserade system. Mykola CHERNYKH är därför inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.	24.6.2024

ELI: http://data.europa.eu/eli/reg_impl/2024/1778/oj

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Födelsedatum: 20.4.1989 Födelseort: Serpukhov, Ryska federationen Nationalitet: rysk Adress: Serpukhov Kön: man	Mikhail Mikhailovich TSAREV var inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot EU:s medlemsstater. Mikhail Mikhailovich TSAREV, som också är känd under internetmonikerna 'Mango', 'Alexander Grachev', 'Super Misha', 'Ivanov Mixail', 'Misha Krutysha' och 'Nikita Andrejevitj Tsarev' är en viktig aktör i användningen av sabotageprogrammen 'Conti' och 'Trickbot' och är inblandad i den Rysslandsbaserade hotgruppen 'Wizard Spider'. Sabotageprogrammen Conti och Trickbot skapades och utvecklades av Wizard Spider. Wizard spider har genomfört kampanjer med utpressningsprogram inom en rad olika sektorer, däribland grundläggande tjänster som hälso- och sjukvård och bankverksamhet. Gruppen har infekterat datorer i hela världen och deras skadliga programvaror har utvecklats till ett mycket modulärt sabotageprogram. Kampanjer som genomförs av Wizard Spider med hjälp av skadliga programvaror som Conti, 'Ryuk' och TrickBot orsakar betydande ekonomiska skador i Europeiska unionen. Mikhail Mikhailovich TSAREV är därför inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.	24.6.2024

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Födelsedatum: 19.5.1982 Födelseort: Abakan, Ryska federationen Nationalitet: rysk Kön: man	Maksim Galochkin var inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot EU:s medlemsstater. Maksim Galochkin är också känd under webbmonikerna 'Benalen', 'Bentley', 'Volhvb', 'volhvb', 'manuel', 'Max17' och 'Crypt'. Galochkin är en viktig aktör i användningen av sabotageprogrammen 'Conti' och 'Trickbot' och är inblandad i den Rysslandsbaserade hotgruppen 'Wizard Spider'. Han har lett en grupp testare med ansvar för utveckling, övervakning och genomförande av tester för sabotageprogrammet TrickBot, som skapats och satts in av Wizard Spider. Wizard Spider har genomfört kampanjer med utpressningsprogram inom en rad olika sektorer, däribland grundläggande tjänster som hälso- och sjukvård och bankverksamhet. Gruppen har infekterat datorer i hela världen och deras skadliga programvaror har utvecklats till ett mycket modulärt sabotageprogram. Kampanjer som genomförs av Wizard Spider med hjälp av skadliga programvaror som Conti, 'Ruyk' och TrickBot orsakar betydande ekonomiska skador i Europeiska unionen. Maksim Galochkin är därför inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.	24.6.2024”

ELI: http://data.europa.eu/eli/reg_impl/2024/1778/oj