2024/1778

24.6.2024

RÅDETS GENNEMFØRELSESFORORDNING (EU) 2024/1778

af 24. juni 2024

om gennemførelse af forordning (EU) 2019/796 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Rådets forordning (EU) 2019/796 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater ([1]), særlig artikel 13, stk. 1,

under henvisning til forslag fra Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, og

ud fra følgende betragtninger:

(1) Den 17. maj 2019 vedtog Rådet forordning (EU) 2019/796.

(2) Målrettede restriktive foranstaltninger til bekæmpelse af cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater, er en af foranstaltningerne i Unionens ramme for en fælles diplomatisk reaktion på ondsindede cyberaktiviteter (»den cyberdiplomatiske værktøjskasse«) og er et afgørende instrument til at forebygge, afskrække fra, modvirke og reagere på sådanne aktiviteter.

(3) Ondsindede cyberaktiviteter mod kritisk infrastruktur eller væsentlige tjenester, herunder gennem brug af ransomware og wipere, rettet mod forsyningskæder og cyberspionage, herunder tyveri af intellektuelle ejendomsrettigheder, er stigende for så vidt angår antal, hyppighed og sofistikeringsgrad. Med deres skadelige og ødelæggende virkninger udgør disse aktiviteter en systemisk trussel mod Unionens sikkerhed, økonomi, demokrati og samfund som helhed.

(4) Brugen af cyberoperationer, der har muliggjort og ledsaget Ruslands uprovokerede og uberettigede angrebskrig mod Ukraine, påvirker den globale stabilitet og sikkerhed, udgør en stor risiko for eskalering og øger den allerede betydelige stigning i ondsindede cyberaktiviteter uden for rammerne af de seneste års væbnede konflikter. De voksende cybersikkerhedsrisici og et generelt komplekst cybertrusselsbillede med en klar risiko for, at cyberhændelser hurtigt spreder sig fra én medlemsstat til andre og fra tredjelande til Unionen, kræver endvidere restriktive foranstaltninger i henhold til forordning (EU) 2019/796.

(5) Som led i den bæredygtige, skræddersyede og koordinerede EU-indsats over for persistente cybertrusselsaktører bør seks fysiske personer opføres på listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, i bilag I til forordning (EU) 2019/796. Disse personer er ansvarlige for eller har været involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.

(6) Bilag I til forordning (EU) 2019/796 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE FORORDNING:

Artikel 1

Bilag I til forordning (EU) 2019/796 ændres som angivet i bilaget til nærværende forordning.

([1]) EUT L 129 I af 17.5.2019, s. 1.

Artikel 2

Denne forordning træder i kraft på dagen for offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Luxembourg, den 24. juni 2024.

På Rådets vegne

J. BORRELL FONTELLES

Formand

BILAG

Følgende punkter tilføjes i afsnit »A. Fysiske personer« i bilag I til forordning (EU) 2019/796:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
»9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Fødselsdato: 3.8.1985 Nationalitet: russisk Køn: mand	Ruslan Peretyatko deltog i cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod Unionen eller dens medlemsstater. Ruslan Peretyatko er en del af »Callisto Group« bestående af russiske militære efterretningsofficerer, der udfører cyberoperationer mod EU-medlemsstater og tredjelande. Callisto Group (alias »Seaborgium«, »Star Blizzard«, »ColdRiver« og »TA446«) har iværksat flerårige phishingkampagner, der anvendes til at stjæle kontobrugeroplysninger og -data. Desuden er Callisto Group ansvarlig for kampagner rettet mod enkeltpersoner og kritiske statslige funktioner, herunder inden for forsvar og eksterne forbindelser. Ruslan Peretyatko er således involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Fødselsdato: 18.5.1987 Fødested: Syktyvkar by, Rusland Nationalitet: russisk Køn: mand	Andrey Stanislavovich Korinets deltog i cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod Unionen eller dens medlemsstater. Andrey Stanislavovich Korinets er officer i »Center 18« i Den Russiske Føderations Føderale Sikkerhedstjeneste (FSB). Andrey Stanislavovich Korinets er en del af »Callisto Group« bestående af russiske militære efterretningsofficerer, der udfører cyberoperationer mod EU-medlemsstater og tredjelande. Callisto Group (alias »Seaborgium«, »Star Blizzard«, »ColdRiver« og »TA446«) har iværksat flerårige phishingkampagner, der anvendes til at stjæle kontobrugeroplysninger og -data. Desuden er Callisto Group ansvarlig for kampagner rettet mod enkeltpersoner og kritiske statslige funktioner, herunder inden for forsvar og eksterne forbindelser. Andrey Stanislavovich Korinets er således involveret i cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (russisk stavemåde) Олександр СКЛЯНКО (ukrainsk stavemåde) Fødselsdato: 5.8.1973 Pasnr.: EC 867868, udstedt den 27.11.1998 (Ukraine) Køn: mand	Oleksandr Sklianko deltog i cyberangreb med betydelige konsekvenser mod EU-medlemsstater samt cyberangreb med betydelige konsekvenser mod tredjelande. Oleksandr Sklianko er en del af hackergruppen »Armageddon«, der støttes af Den Russiske Føderations Føderale Sikkerhedstjeneste (FSB), og som gennemførte en række cyberangreb med betydelige konsekvenser mod Ukraines regering og mod EU-medlemsstater og deres regeringsembedsmænd, herunder ved at anvende phishingmails og malwarekampagner. Oleksandr Sklianko er således involveret i cyberangreb med betydelige konsekvenser mod tredjelande samt cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (russisk stavemåde) Микола ЧЕРНИХ (ukrainsk stavemåde) Fødselsdato: 12.10.1978 Pasnr.: EC 922162, udstedt den 20.1.1999 (Ukraine) Køn: mand	Mykola Chernykh deltog i cyberangreb med betydelige konsekvenser mod EU-medlemsstater samt cyberangreb med betydelige konsekvenser mod tredjelande. Mykola Chernykh er en del af hackergruppen »Armageddon«, der støttes af Den Russiske Føderations Føderale Sikkerhedstjeneste (FSB), og som gennemførte en række cyberangreb med betydelige konsekvenser mod Ukraines regering og mod EU-medlemsstater og deres regeringsembedsmænd, herunder ved at anvende phishingmails og malwarekampagner. Som tidligere ansat i Ukraines sikkerhedstjeneste er han i Ukraine tiltalt for forræderi og uautoriserede indgreb i driften af elektroniske databehandlingsmaskiner og automatiserede systemer. Mykola Chernykh er således involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Fødselsdato: 20.4.1989 Fødested: Serpukhov, Den Russiske Føderation Nationalitet: russisk Adresse: Serpukhov Køn: mand	Mikhail Mikhailovich Tsarev deltog i cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod EU-medlemsstater. Mikhail Mikhailovich Tsarev, som også er kendt under internettilnavnet »Mango«, »Alexander Grachev«, »Super Misha«, »Ivanov Mixail«, »Misha Krutysha« og »Nikita Andreevich Tsarev«, er en central aktør i deployeringen af »Conti« og »Trickbot« malware programmer, og er involveret i den Rusland-baserede trussel gruppe »Wizard Spider«. De af Conyi og Trickbot anvendte malware programmer var oprettet og udviklet af Wizard Spider. Wizard Spider har gennemført ransomwarekampagner i en række sektorer, herunder vigtige tjenester såsom sundhed og bankvæsen. Gruppen har inficeret computere verden over, og dens malware er blevet udviklet til en meget modulær malwarepakke. De kampagner, der gennemføres af Wizard Spider, som bruger malware såsom Conti, »Ryuk« og TrickBot, er skyld i omfattende økonomisk skade i Den Europæiske Union. Mikhail Mikhailovich Tsarev er således involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Fødselsdato: 19.5.1982 Fødested: Abakan, Den Russiske Føderation Nationalitet: russisk Køn: mand	Maksim Galochkin deltog i cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod EU-medlemsstater. Maksim Galochkin er også kendt under internettilnavnene »Benalen«, »Bentley«, »Volhvb«, »volhvb«, »manuel«, »Max17« og »Crypt«. Galochkin er en central aktør i deployeringen af »Conti« og »TrickBot« malware programmer, og er involveret i den Rusland-baserede trussel gruppe »Wizard Spider«. Han har stået i spidsen for en gruppe testere med ansvar for udviklingen af, tilsyn med og gennemførelse af test af TrickBot-spywareprogrammet, der er udviklet og anvendt af Wizard Spider. Wizard Spider har gennemført ransomwarekampagner i en række sektorer, herunder vigtige tjenester såsom sundhed og bankvæsen. Gruppen har inficeret computere verden over, og dens malware er blevet udviklet til en meget modulær malwarepakke. De kampagner, der gennemføres af Wizard Spider, som bruger malware såsom Conti, »Ryuk« og TrickBot, er skyld i omfattende økonomisk skade i Den Europæiske Union. Maksim Galochkin er således involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024«