Conselho
da União Europeia

Bruxelas, 7 de julho de 2026
(OR. en)

8645/26

LIMITE

CORLX 390
CFSP/PESC 586
RELEX 561
CYBER 194
JAI 507
FIN 594

ATOS LEGISLATIVOS E OUTROS INSTRUMENTOS

Assunto:	REGULAMENTO DE EXECUÇÃO DO CONSELHO que dá execução ao Regulamento (UE) 2019/796 relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros

REGULAMENTO DE EXECUÇÃO (UE) 2026/… DO CONSELHO

de …

que dá execução ao Regulamento (UE) 2019/796 relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2019/796 do Conselho, de 17 de maio de 2019, relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros[1], nomeadamente o artigo 13.º, n. 1,

Tendo em conta a proposta da alta representante da União para os Negócios Estrangeiros e a Política de Segurança,

[1] JO L 129I de 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

Considerando o seguinte:

(1) Em 17 de maio de 2019, o Conselho adotou o Regulamento (UE) 2019/796.

(2) No âmbito da ação sustentada, adaptada e coordenada da União contra os responsáveis por ciberameaças persistentes, oito pessoas singulares e quatro entidades deverão ser aditadas à lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas constante do anexo I do Regulamento (UE) 2019/796. Essas pessoas e entidades são responsáveis ou estão envolvidas em ciberataques com um efeito significativo que constituem uma ameaça externa para a União ou os seus Estados-Membros.

(3) Por conseguinte, o anexo I do Regulamento (UE) 2019/796 deverá ser alterado em conformidade,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

O anexo I do Regulamento (UE) 2019/796 é alterado nos termos do anexo do presente regulamento.

Artigo 2.º

O presente regulamento entra em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em …, em

Pelo Conselho
O Presidente / A Presidente

ANEXO

O anexo I do Regulamento (UE) 2019/796 é alterado do seguinte modo:

1) À rubrica «A. Pessoas singulares» são aditadas as seguintes entradas:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Pseudónimos: «Bentley», «Bergen», «Alex Konor», «Benny», «Ben», «Stern» Data de nascimento: 23.6.1988 Endereço: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg, Federação da Rússia Nacionalidade: russa Sexo: masculino Entidades associadas: TrickBot, Wizard Spider, Conti	Vitaly Kovalev é um dos principais responsáveis pelos programas maliciosos «Trickbo»" e «Conti». É também conhecido pelos pseudónimos virtuais «Bentley», «Bergen», «Alex Konor», «Benny», «Ben» e «Stern». Os programas Conti e Trickbot foram criados e desenvolvidos pelo grupo Wizard Spider. O grupo Wizard Spider levou a cabo campanhas com programas sequestradores em diferentes setores, nomeadamente em serviços essenciais como os da saúde e da banca, tem infetado computadores em todo o mundo e os seus programas maliciosos foram desenvolvidos de forma a tornarem-se uma série de programas maliciosos altamente modular. As campanhas do Wizard Spider com recurso a programas maliciosos, como o Conti e o TrickBot, são responsáveis por prejuízos económicos substanciais na União Europeia. Por conseguinte, Vitaly Kovalev está implicado e é responsável por ciberataques com um efeito significativo que constituem uma ameaça externa para a União ou os seus Estados-Membros.	[+]

[+] JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Data de nascimento: 30.1.1983 Local de nascimento: URSS Nacionalidade: russa Número de passaporte: 762988138 Sexo: masculino Entidades associadas: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik é o proprietário da Media Land LLC. Desde 2016, a Media Land LLC, que presta serviços de alojamento blindado («bulletproof hosting»), tem facilitado uma vasta gama de ataques com programas maliciosos contra a União e a nível mundial, oferecendo serviços de alojamento virtual que ocultam a identidade dos utilizadores e resistem às ordens de remoção de conteúdos das autoridades policiais. A Media Land LLC viabilizou operações em grande escala com programas sequestradores, serviços de comando e controlo e operações de mistificação da interface que visam infraestruturas críticas e serviços essenciais nos Estados-Membros, causando perdas financeiras significativas. A Media Land LLC facilita, nomeadamente, as operações dos grupos LockBit, EvilCorp e BlackBasta. Por conseguinte, a Media Land LLC está envolvida em ciberataques com um efeito significativo que constituem uma ameaça externa para a União ou os seus Estados-Membros. Sendo proprietário da Media Land LLC, Alexander Volosovik é responsável por estes ciberataques e está neles envolvido. Está também associado à Media Land LLC.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Pseudónimo: «Dena» Data de nascimento: 9.10.1989 Local de nascimento: URSS Nacionalidade: russa Sexo: masculino Endereço: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Federação da Rússia	Denis Degtyarenko, também conhecido por «Dena», é um pirata informático russo do grupo CARR («Cyber Army of Russia Reborn»). O CARR é responsável por ciberataques contra serviços necessários para a manutenção de atividades económicas essenciais e funções críticas do Estado nos Estados-Membros, bem como contra infraestruturas na Ucrânia e noutros países terceiros. O CARR está associado ao Main Centre for Special Technologies (GTsST) within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [Centro Principal de Tecnologias Especiais (GTsST) no seio da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GRU)]. O GTsST continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Os alvos do CARR incluem agências governamentais, instituições financeiras, meios de comunicação social e infraestruturas críticas nos Estados-Membros e nos Estados Unidos. O CARR levou a cabo ataques distribuídos de negação de serviço contra a Ucrânia e contra governos e empresas localizados em países que apoiaram a Ucrânia. Por conseguinte, Denis Degtyarenko, um dos principais piratas informáticos do CARR, está envolvido em ciberataques com um efeito significativo, incluindo tentativas de ciberataque com um efeito potencialmente significativo, que constituem uma ameaça externa para os Estados-Membros, bem como para Estados terceiros. Enquanto membro do CARR, está também associado ao GTsST.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Pseudónimo: "YUliYA" Data de nascimento: 6.4.1984 Local de nascimento: URSS Nacionalidade: russa Sexo: feminino Endereço: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Federação da Rússia	Yuliya Pankratova é uma pirata informática russa que tem trabalhado para o CARR (Cyber Army of Russia Reborn) e que fundouo grupo Z-Pentest, para o qual continua a trabalhar. O CARR é responsável por ciberataques contra serviços necessários para a manutenção de atividades económicas essenciais e funções críticas do Estado nos Estados-Membros, bem como contra infraestruturas na Ucrânia e noutros países terceiros. O CARR está associado ao Main Centre for Special Technologies (GTsST) within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [Centro Principal de Tecnologias Especiais (GTsST) no seio da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GRU)]. O GTsST continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Os alvos do CARR incluem agências governamentais, instituições financeiras, meios de comunicação social e infraestruturas críticas nos Estados-Membros e nos Estados Unidos. O CARR levou a cabo ataques distribuídos de negação de serviço contra a Ucrânia e contra governos e empresas localizados em países que apoiaram a Ucrânia.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			O Z-Pentest é responsável por ciberataques com um efeito significativo, nomeadamente por ciberataques contra serviços necessários para a manutenção de atividades essenciais nos Estados-Membros. Por conseguinte, Yuliya Pankratova, uma das principais piratas informáticas do CARR e do Z-Pentest, está envolvida em ciberataques com um efeito significativo, incluindo tentativas de ciberataque com um efeito potencialmente significativo, que constituem uma ameaça externa para os Estados-Membros, bem como para Estados terceiros. Está também associada ao Z-Pentest.	

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Pseudónimo: «Daugn0» Nacionalidade: presumivelmente russa Sexo: masculino	Maksim Voronin, também conhecido por «Daugn0», está envolvido no desenvolvimento, distribuição e venda do programa malicioso de roubo de informação LummaC2 (também conhecido por «Lumma infostealer» e «Lumma Stealer»). O LummaC2 consiste numa plataforma de programas maliciosos como serviço («MaaS») utilizada para roubar dados sensíveis, credenciais armazenadas em navegadores, carteiras de criptoativos ou informações de sistemas, a fim de implantar outros programas maliciosos nos dispositivos infetados, roubar criptomoedas e realizar campanhas de espionagem. Os ciberataques com o programa malicioso LummaC2 são também utilizados por perpetradores de ciberameaças com motivações financeiras, como o Storm-113, o Storm-1607, o Storm-1674, o Octo Tempest, entre outros. O programa malicioso LummaC2 tem sido utilizado para ciberataques contra funções críticas do Estado e serviços necessários para a manutenção de atividades sociais e económicas essenciais dos Estados-Membros. Em 2024 e 2025, o LummaC2 foi uma das ferramentas mais utilizadas para roubar informações em todo o mundo. Por conseguinte, Maksim Voronin, enquanto criador, distribuidor e vendedor do LummaC2, está envolvido e facilita ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
25.	Maksim Aleksandrovich GORDIENKO t.c.p. Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Pseudónimo: «Lummaseller» Nacionalidade: presumivelmente russa Sexo: masculino	Maksim Gordienko, também conhecido por «Lummaseller», está envolvido no desenvolvimento e distribuição do programa malicioso de roubo de informação LummaC2 (também conhecido por «Lumma infostealer» e «Lumma Stealer»). O LummaC2 consiste numa plataforma de programas maliciosos como serviço («MaaS») utilizada para roubar dados sensíveis, credenciais armazenadas em navegadores, carteiras de criptoativos ou informações de sistemas, a fim de implantar outros programas maliciosos nos dispositivos infetados, roubar criptomoedas e realizar campanhas de espionagem. Os ciberataques com o programa malicioso LummaC2 são também utilizados por perpetradores de ciberameaças com motivações financeiras, como o Storm-113, o Storm-1607, o Storm-1674, o Octo Tempest, entre outros. O programa malicioso LummaC2 tem sido utilizado para ciberataques contra funções críticas do Estado e serviços necessários para a manutenção de atividades sociais e económicas essenciais dos Estados-Membros. Em 2024 e 2025, o LummaC2 foi uma das ferramentas mais utilizadas para roubar informações em todo o mundo. Por conseguinte, Maksim Gordienko, enquanto criador, distribuidor e vendedor do LummaC2, está envolvido e facilita ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Data de nascimento: 25.1.1980 Local de nascimento: URSS Nacionalidade: russa Sexo: masculino Pessoas associadas: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Entidades associadas: Unidade 29155 da GRU, «Impuls» LLC	Evgeniy Bashev é membro da Unidade 29155 da GRU, agência de informações militares russa. Na unidade, apoia e facilita ciberataques com um efeito significativo contra os Estados-Membros, nomeadamente através do controlo do servidor «Aegon», utilizado para operações de pirataria informática. Em especial, presta apoio técnico e material aos ciberataques da Unidade 29155 da GRU através da sua empresa «Impuls» LLC, que facilitou a cobertura operacional, as infraestruturas e os pagamentos e geriu os ativos técnicos, nomeadamente servidores, utilizados nos ciberataques. Coordenou igualmente a cooperação entre as estruturas da GRU e as redes externas de piratas informáticos. Os ciberataques que facilitou visaram sistemas de funções críticas do Estado e serviços necessários para a manutenção de atividades sociais ou económicas essenciais nos Estados-Membros, nomeadamente no setor dos transportes. Através da campanha WhisperGate, a Unidade 29155 do GRU visou igualmente infraestruturas críticas da Ucrânia.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			Por conseguinte, Evgeniy Bashev presta apoio técnico e material ou está envolvido de outra forma em ciberataques com um efeito significativo, incluindo tentativas de ciberataque com um efeito potencialmente significativo, que constituem uma ameaça externa para os Estados-Membros, assim como em ciberataques com um efeito significativo contra um país terceiro. Sendo proprietário e diretor-geral da «Impuls» LLC, está associado a essa empresa. Sendo membro da Unidade 29155 da GRU, está também associado a essa entidade.	

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Local de nascimento: Federação da Rússia Nacionalidade: russa Sexo: masculino Pessoas associadas: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Entidades associadas: Unidade 29155 da GRU	Roman Puntus é membro da Unidade 29155 da GRU, agência de informações militares russa. Desempenha, na unidade, um papel de liderança na organização e na coordenação de ciberataques com um efeito significativo contra os Estados-Membros. Apoia igualmente o desenvolvimento da cibercapacidade interna da unidade, nomeadamente no recrutamento e na supervisão do pessoal, incluindo piratas informáticos e programadores. Facilitou, com a criação da empresa de fachada «Aegeon-Impulse», os aspetos logísticos e financeiros das ciberoperações. Sob a sua coordenação, a unidade levou a cabo ciberataques que visaram sistemas de funções críticas do Estado e serviços necessários para a manutenção de atividades sociais ou económicas essenciais nos Estados-Membros, nomeadamente no setor dos transportes. Através da campanha WhisperGate, a Unidade 29155 do GRU visou igualmente infraestruturas críticas da Ucrânia.	[+]»;

[+] JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			Por conseguinte, Roman Puntus é responsável ou está de envolvido de outra forma em ciberataques com um efeito significativo, incluindo tentativas de ciberataque com um efeito potencialmente significativo, que constituem uma ameaça externa para os Estados-Membros, assim como em ciberataques com um efeito significativo contra um país terceiro. Sendo membro da Unidade 29155 da GRU, está também associado a essa entidade.	

2) À rubrica «B. Pessoas coletivas, entidades e organismos» são aditadas as seguintes entradas:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«8.	Media Land LLC	Endereço: Tsvetnochnaya st., 16 Litera P, Room 27 Moskovskaya Zastava Municipal District St Petersburg, 196006, Federação da Rússia Tipo de entidade: Sociedade de responsabilidade limitada Local de registo: São Petersburgo Data de registo: 19.10.2015 Número de registo: 1152536009900 Estabelecimento principal: São Petersburgo, Federação da Rússia Entidade associada: ML.Cloud	Desde 2016, a Media Land LLC, que presta serviços de alojamento blindado («bulletproof hosting»), tem facilitado uma vasta gama de ataques com programas maliciosos contra Estados-Membros e a nível mundial, oferecendo serviços de alojamento virtual que ocultam a identidade dos utilizadores e resistem às ordens de remoção de conteúdos das autoridades policiais, causando perdas financeiras significativas. A Media Land LLC viabilizou operações em grande escala com programas sequestradores, serviços de comando e controlo e operações de mistificação da interface que visam infraestruturas críticas e serviços essenciais nos Estados-Membros. A Media Land LLC facilita, nomeadamente, as operações dos grupos LockBit, EvilCorp e BlackBasta. Por conseguinte, a Media Land LLC está envolvida em ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
9.	ML.Cloud	Endereço: Brivibas iela 52, Riga, LV-1011, Latvija; Federação da Rússia, Kazan, Peterburgskaya st. 52 Local de registo: Riga Pessoa associada: Alexander Volosovik Outras entidades associadas: Media Land LLC	A ML.Cloud é cofilial da Media Land LLC, fornecendo-lhe a infraestrutura técnica. Desde 2016, a Media Land LLC, que presta serviços de alojamento blindado («bulletproof hosting»), tem facilitado uma vasta gama de ataques com programas maliciosos contra Estados-Membros e a nível mundial, oferecendo serviços de alojamento virtual que ocultam a identidade dos utilizadores e resistem às ordens de remoção de conteúdos das autoridades policiais, causando perdas financeiras significativas. A Media Land LLC viabilizou operações em grande escala com programas sequestradores, serviços de comando e controlo e operações de mistificação da interface que visam infraestruturas críticas e serviços essenciais nos Estados-Membros. A Media Land LLC facilita, nomeadamente, as operações dos grupos LockBit, EvilCorp e BlackBasta. Por conseguinte, a Media Land LLC está envolvida em ciberataques que constituem uma ameaça externa com um efeito significativo para os Estados-Membros da UE. Por conseguinte, a ML. Cloud presta apoio técnico a ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
10.	«Impuls» LLC	Общество с ограниченной ответственностью "Импульс" Endereço: 344015, Federação da Rússia, Rostov Region, Rostov-on--Don, ul. Eremenko, d. 56, k. 6, apt. 88 Tipo de entidade: Sociedade de responsabilidade limitada Local de registo: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Federação da Rússia Data de registo: 27.9.2010	A «Impuls» LLC é uma empresa russa detida por Evgeniy Viktorovich Bashev, membro da Unidade 29155 da GRU, agência de informações militares russa. A empresa presta apoio técnico e material a ciberataques e tentativas de ciberataque realizados pela Unidade 29155 da GRU. Em especial, a «Impuls» LLC funciona como intermediário operacional, viabilizando a realização de atividades relacionadas com a pirataria informática através de uma empresa que formalmente não está ligada ao Estado russo. Facilitou a cobertura operacional, as infraestruturas e os pagamentos de ciberataques e esteve ligada a ativos técnicos, nomeadamente servidores, utilizados para apoiar atividades de pirataria informática. Em especial, a «Impuls» LLC permitiu a cooperação entre as estruturas da GRU e as redes externas de piratas informáticos. As ciberoperações facilitadas pela «Impuls» LLC visam funções críticas do Estado e serviços necessários para a manutenção de atividades sociais e económicas essenciais nos Estados-Membros, inclusive no setor dos transportes. Através da campanha WhisperGate, a Unidade 29155 do GRU visou igualmente infraestruturas críticas da Ucrânia.	+

+ JO: inserir a data de publicação do presente regulamento.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
		Número de registo: INN («ИНН», número de identificação fiscal): 6168033776; OGRN («ГРН» número principal de registo nacional): 1106194004850 Estabelecimento principal: Federação da Rússia Pessoas associadas: Evgeniy Bashev Entidades associadas: Unidade 29155 da GRU	Por conseguinte, a «Impuls» LLC presta apoio técnico e material ou está envolvida de outra forma em ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros, assim como em ciberataques com um efeito significativo contra um país terceiro.	

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
11.	Z-Pentest	Pseudónimos: «Z-Pentest Alliance», «Z-Alliance» Estabelecimento principal: Federação da Rússia Pessoas associadas: Yuliya Pankratova Entidades associadas: Cyber Army of Russia/CARR Conta no X.com: ZPentest (conta suspensa) Conta no Telegram: Zpentestalliance	O Z-Pentest é um grupo pró-russo de piratas informáticos ativistas («hacktivists») composto por membros dos grupos CARR («Cyber Army of Russia Reborn») e NoName057 que visa infraestruturas críticas a nível mundial, especialmente no setor da energia e da água. O grupo atacou, nomeadamente, uma empresa de distribuição de água dinamarquesa em dezembro de 2024. Por conseguinte, o Z-Pentest é responsável por ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros.	[+]».

[+] JO: inserir a data de publicação do presente regulamento.