2026/1078

12.5.2026

REGULAMENTO DE EXECUÇÃO (UE) 2026/1078 DO CONSELHO

de 11 de maio de 2026

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,

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

Considerando o seguinte:

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

(2) O Conselho procedeu a uma reapreciação da lista de pessoas singulares e coletivas, entidades e organismos constante do anexo I do Regulamento (UE) 2019/796. Com base na referida reapreciação, deverão ser atualizados os motivos da inclusão de quatro pessoas e uma entidade na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas.

(3) O anexo I do Regulamento (UE) 2019/796 deverá, pois, 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 seguinte ao 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 Bruxelas, em 11 de maio de 2026.

Pelo Conselho

A Presidente

K. KALLAS

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

ANEXO

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

1) Na secção «A. Pessoas singulares», as entradas 1, 2, 13 e 14 são substituídas pelas seguintes entradas correspondentes:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«1.	GAO Qiang	Data de nascimento: 4 de outubro de 1983 Local de nascimento: Província de Shandong, China Endereço: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nacionalidade: chinesa Sexo: masculino	Gao Qiang está ligado ao grupo "APT10" ("Advanced Persistent Threat 10") (t.c.p. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") e esteve envolvido na "Operação Cloud Hopper", uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A "Operação Cloud Hopper" atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. GAO Qiang está associado à infraestrutura de comando e controlo do "APT10". Além disso, a Huaying Haitai, uma empresa utilizada pelo "APT10" e designada por apoiar e facilitar a "Operação Cloud Hopper", empregou Gao Qiang. Este também está associado a Zhang Shilong, que tem ligação ao "APT10" e também foi empregado da Huaying Haitai.	30.7.2020

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
2.	ZHANG Shilong	Data de nascimento: 10 de setembro de 1981 Local de nascimento: China Endereço: Hedong, Yuyang Road No 121, Tianjin, China Nacionalidade: chinesa Sexo: masculino	Zhang Shilong está ligado ao grupo "APT10" ("Advanced Persistent Threat 10") (t.c. p. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") e esteve envolvido na "Operação Cloud Hopper", uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A "Operação Cloud Hopper" atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. Zhang Shilong está associado ao "APT10", nomeadamente através do programa malicioso que desenvolveu e testou em ligação com os ciberataques lançados pelo "APT10". Além disso, a Huaying Haitai, uma empresa utilizada pelo "APT10" e designada por apoiar e facilitar a "Operação Cloud Hopper", empregou Zhang Shilong. Este está associado a Gao Qiang, que tem ligação ao "APT10" e também foi empregado da Huaying Haitai.	30.7.2020

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data de nascimento: 20.4.1989 Local de nascimento: Serpukhov, Federação da Rússia Nacionalidade: russa Endereço: Serpukhov Sexo: masculino	Mikhail Mikhailovich TSAREV participou em ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros da UE. Mikhail Mikhailovich TSAREV, também conhecido pelos nomes em linha "Mango", "Alexander Grachev", "Super Misha", "Ivanov Mixail", "Misha Krutysha" e "Nikita Andreevich Tsarev", é um interveniente fundamental na implementação dos programas maliciosos "Conti" e "Trickbot", e está envolvido no grupo de ameaça "Wizard Spider" baseado na Rússia. O "Wizard Spider" continua a evoluir e a intensificar as suas operações. Os programas maliciosos "Conti" e "Trickbot" foram criados e desenvolvidos pelo "Wizard Spider". O grupo "Wizard Spider" empreendeu campanhas com programas sequestradores em diversos setores, nomeadamente em serviços essenciais como a saúde e a banca. O grupo 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 grupo "Wizard Spider" com recurso a programas maliciosos, como "Conti", "Ryuk", "TrickBot" ou "Black Basta", são responsáveis por prejuízos económicos substanciais na União Europeia. Por conseguinte, Mikhail Mikhailovich TSAREV está envolvido em ciberataques com um efeito significativo que constituem uma ameaça externa para a União ou os seus Estados-Membros.	24.6.2024

ELI: http://data.europa.eu/eli/reg_impl/2026/1078/oj

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data de nascimento: 19.5.1982 Local de nascimento: Abakan, Federação da Rússia Nacionalidade: russa Sexo: masculino	Maksim GALOCHKIN participou em ciberataques com um efeito significativo que constituem uma ameaça externa para os Estados-Membros da UE. Maksim GALOCHKIN é também conhecido pelos nomes em linha "Benalen", "Bentley", "Volhvb", "volhvb", "Manuel", "Max17" e "Crypt". Maksim GALOCHKIN é um interveniente fundamental na implementação dos programas maliciosos "Conti" e "Trickbot", e está envolvido no grupo de ameaça "Wizard Spider" baseado na Rússia. Liderou um grupo de testadores, responsáveis por desenvolver, supervisionar e executar os testes para o programa malicioso "TrickBot", criado e implementado pelo "Wizard Spider". O "Wizard Spider" continua a evoluir e a intensificar as suas operações. O grupo "Wizard Spider" empreendeu campanhas com programas sequestradores em diversos setores, nomeadamente em serviços essenciais como a saúde e a banca. O grupo 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 grupo "Wizard Spider", com recurso a programas maliciosos como "Conti", "Ryuk", "TrickBot" ou "Black Basta", são responsáveis por prejuízos económicos substanciais na União Europeia. Por conseguinte, Maksim GALOCHKIN está envolvido em ciberataques com um efeito significativo que constituem uma ameaça externa para a União ou os seus Estados-Membros.	24.6.2024»;

2) Na secção «B. Pessoas coletivas, entidades e organismos», a entrada 1 passa a ter a seguinte redação:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	t.c.p. Haitai Technology Development Co. Ltd Localização: Tianjin, China	A Huaying Haitai prestou apoio financeiro, técnico ou material e facilitou a "Operação Cloud Hopper", uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A "Operação Cloud Hopper" atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. O interveniente conhecido por "APT10" ("Advanced Persistent Threat 10") (t.c.p. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") realizou a "Operação Cloud Hopper". Pode estabelecer-se uma ligação entre a Huaying Haitai e o "APT10". Além disso, a Huaying Haitai empregou Gao Qiang e Zhang Shilong, ambos designados pela sua ligação à "Operação Cloud Hopper". Por conseguinte, a Huaying Haitai também está associada a Gao Qiang e a Zhang Shilong.	30.7.2020».

ELI: http://data.europa.eu/eli/reg_impl/2026/1078/oj