2026/1713

2026.7.13.

A TANÁCS (KKBP) 2026/1713 HATÁROZATA

(2026. július 13.)

az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (KKBP) 2019/797 határozat módosításáról

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unióról szóló szerződésre és különösen annak 29. cikkére,

tekintettel az Unió külügyi és biztonságpolitikai főképviselőjének javaslatára,

mivel:

(1) A Tanács 2019. május 17-én elfogadta a (KKBP) 2019/797 határozatot [1].

(2) A tartós kiberfenyegetés mögött álló szereplőkkel szembeni lankadatlan, személyre szabott és koordinált uniós fellépés részeként nyolc természetes személyt és négy szervezetet fel kell venni a korlátozó intézkedések hatálya alá tartozó természetes és jogi személyeknek, szervezeteknek és szerveknek a (KKBP) 2019/797 határozat mellékletében foglalt jegyzékébe. Az említett személyek és szervezetek felelősek olyan jelentős hatású kibertámadásokért, amelyek az Unióra vagy a tagállamaira nézve külső fenyegetést jelentenek, vagy részt vesznek azokban.

(3) A (KKBP) 2019/797 határozatot ezért ennek megfelelően módosítani kell,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A (KKBP) 2019/797 határozat melléklete e határozat mellékletének megfelelően módosul.

2. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

Kelt Brüsszelben, 2026. július 13-án.

a Tanács részéről

az elnök

K. KALLAS

[1] A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről (HL L 129I., 2019.5.17., 13. o., ELI: http://data.europa.eu/eli/dec/2019/797/oj).

MELLÉKLET

A (KKBP) 2019/797 határozat melléklete a következőképpen módosul:

1. Az „A. Természetes személyek” cím alatt a szöveg a következő bejegyzésekkel egészül ki:

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ más néven: »Bentley«, »Bergen«, »Alex Konor«, »Benny«, »Ben«, »Stern« Születési idő: 1988.6.23. Cím: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Állampolgárság: orosz Nem: férfi Kapcsolódó szervezetek: TrickBot, Wizard Spider, Conti	Vitaly Kovalev vezető szerepet tölt be a »Trickbot« és a »Conti« rosszindulatú programokkal összefüggésben. A »Bentley«, »Bergen«, »Alex Konor«, »Benny«, »Ben« és »Stern« internetes azonosítóneveken is ismert. A Contit és a Trickbotot eredetileg a Wizard Spider hozta létre. A Wizard Spider számos ágazatban, többek között az olyan alapvető szolgáltatások vonatkozásában folytatott zsarolóvírus-kampányokat, mint például az egészségügy és a bankolás, számítógépeket fertőzött meg világszerte, és rosszindulatú szoftvereit egy rendkívül moduláris rosszindulatúszoftver-csomaggá fejlesztette. A Wizard Spider által olyan rosszindulatú szoftverek használatával folytatott kampányok, mint például a Conti és a TrickBot, jelentős gazdasági kárt okoznak az Európai Unióban. Vitaly Kovalevet ennélfogva felelősség terheli jelentős hatású, az Unió vagy a tagállamai számára külső fenyegetést jelentő kibertámadásokért, illetve részt vesz azokban.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Születési idő: 1983.1.30. Születési hely: USSR Állampolgárság: orosz Útlevélszám: 762988138 Nem: férfi Kapcsolódó szervezetek: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik a Media Land LLC tulajdonosa. 2016 óta a Bullet Proof Hosting Service Media Land LLC rosszindulatú szoftverrel elkövetett támadások széles körét segíti elő mind az Unió ellen, mind pedig világszerte azáltal, hogy olyan tárhelyszolgáltatásokat kínál, amelyek segítségével elrejtik a felhasználói azonosítókat és kivédik tartalmaknak a bűnüldöző szervek általi eltávolítását. A Media Land LLC olyan nagyszabású zsarolóvírus-műveleteket, irányítási és vezérlési szolgáltatásokat, valamint adathalászatra irányuló műveleteket tett lehetővé, amelyek kritikus infrastruktúrákat és alapvető szolgáltatásokat vesznek célba a tagállamokban, jelentős pénzügyi veszteségeket okozva. A Media Land LLC által elősegített műveletek közé tartozik többek között a LockBit, az EvilCorp és a BlackBasta. A Media Land LLC tehát olyan jelentős hatású kibertámadásokban vesz részt, amelyek külső fenyegetést jelentenek az Unió vagy a tagállamai számára. A Media Land LLC tulajdonosaként Alexander Volosovikot felelősség terheli e kibertámadásokért, és részt vesz azokban. Kapcsolatban áll a Media Land LLC-vel is.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО más néven: »Dena« Születési idő: 1989.10.9. Születési hely: USSR Állampolgárság: orosz Nem: férfi Cím: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko más néven Dena a CARR (Cyber Army of Russia Reborn) orosz hekkere. A CARR-t felelősség terheli olyan kibertámadásokért, amelyek a tagállamokban az alapvető gazdasági tevékenységek és kritikus állami funkciók fenntartásához szükséges szolgáltatások, valamint az ukrajnai és más harmadik országbeli infrastruktúra ellen irányultak. A CARR kapcsolatban áll az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságán (Main Directorate of the General Staff of the Armed Forces of the Russian Federation, GRU) belül működő Különleges Technológiai Főközponttal (Main Centre for Special Technologies, GTsST). A GTsST továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. A CARR célpontjai közé tartoznak a tagállamokban és az Egyesült Államokban működő kormányzati ügynökségek, pénzügyi intézmények, médiaorgánumok és kritikus infrastruktúrák. A CARR elosztott szolgáltatásmegtagadásos (DDoS) támadásokat hajtott végre Ukrajnában, valamint az Ukrajnát támogató országokban található kormányok és vállalatok ellen. Ezért Denis Degtyarenko, a CARR egyik fontos hekkere olyan, jelentős hatású kibertámadásokban – többek között potenciálisan jelentős hatású kibertámadási kísérletekben – vesz részt, amelyek külső fenyegetést jelentenek a tagállamok, valamint harmadik államok számára. Kapcsolatban áll a GTsST-vel is, mint annak tagja.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА más néven: »YUliYA« Születési idő: 1984.4.6. Születési hely: USSR Állampolgárság: orosz Nem: nő Cím: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova orosz hekker, aki a CARR-nak (Cyber Army of Russia Reborn) dolgozott, és megalapította a Z-Pentestet, amelynek továbbra is dolgozik. A CARR-t felelősség terheli olyan kibertámadásokért, amelyek a tagállamokban az alapvető gazdasági tevékenységek és kritikus állami funkciók fenntartásához szükséges szolgáltatások, valamint az ukrajnai és más harmadik országbeli infrastruktúra ellen irányultak. A CARR kapcsolatban áll az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságán (Main Directorate of the General Staff of the Armed Forces of the Russian Federation, GRU) belül működő Különleges Technológiai Főközponttal (Main Centre for Special Technologies, GTsST). A GTsST továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. A CARR célpontjai közé tartoznak a tagállamokban és az Egyesült Államokban működő kormányzati ügynökségek, pénzügyi intézmények, médiaorgánumok és kritikus infrastruktúrák. A CARR elosztott szolgáltatásmegtagadásos (DDoS) támadásokat hajtott végre Ukrajnában, valamint az Ukrajnát támogató országokban található kormányok és vállalatok ellen. A Z-Pentestet felelősség terheli olyan kibertámadásokért, amelyek jelentős hatást gyakorolnak többek között a tagállamokban az alapvető tevékenységek fenntartásához szükséges szolgáltatásokra. Ezért Yuliya Pankratova, a CARR és a Z-Pentest egyik fontos hekkere olyan, jelentős hatású kibertámadásokban – többek között potenciálisan jelentős hatású kibertámadási kísérletekben – vesz részt, amelyek külső fenyegetést jelentenek a tagállamok, valamint harmadik államok számára. Kapcsolatban áll a Z-Pentesttel is.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН más néven: »Daugn0« Állampolgárság: állítólagosan orosz Nem: férfi	Maksim Voronin más néven Daugn0 részt vesz a LummaC2 (más néven Lumma Infostealer, Lumma Stealer) elnevezésű, információk ellopására szolgáló rosszindulatú szoftver fejlesztésében, terjesztésében és értékesítésében. A LummaC2 olyan Malware-as-a-Service (MaaS) platform, amelyet érzékeny adatoknak, böngészők hitelesítési adatainak, kriptotárcáknak vagy rendszerinformációknak az ellopására, további rosszindulatú szoftverek fertőzött eszközökön való telepítésére, kriptovaluta-lopásra és kémkedési kampányokra használnak. A LummaC2 rosszindulatú szoftver használatával elkövetett kibertámadásokat többek között olyan pénzügyi indíttatású, kiberfenyegetés mögött álló szereplők is használják, mint a Storm-113, a Storm-1607, a Storm-1674 és az Octo Tempest. A LummaC2 rosszindulatú szoftvert felhasználják a tagállamok alapvető társadalmi és gazdasági tevékenységeinek fenntartásához szükséges kritikus állami funkciók és szolgáltatások elleni kibertámadásokhoz. 2024-ben és 2025-ben a LummaC2 világszerte az információk ellopására leggyakrabban használt eszközök egyike volt. Ezért Maksim Voronin a LummaC2 fejlesztőjeként, forgalmazójaként és értékesítőjeként olyan, jelentős hatású kibertámadásokban vesz részt – és segíti elő azokat –, amelyek külső fenyegetést jelentenek a tagállamok számára.	2026.7.13.

ELI: http://data.europa.eu/eli/dec/2026/1713/oj

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
25.	Maksim Aleksandrovich GORDIENKO más néven: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО más néven: »Lummaseller« Állampolgárság: állítólagosan orosz Nem: férfi	Maksim Gordienko más néven Lummaseller részt vesz a LummaC2 (más néven Lumma Infostealer, Lumma Stealer) elnevezésű, információk ellopására szolgáló rosszindulatú szoftver fejlesztésében és terjesztésében. A LummaC2 olyan Malware-as-a-Service (MaaS) platform, amelyet érzékeny adatoknak, böngészők hitelesítési adatainak, kriptotárcáknak vagy rendszerinformációknak az ellopására, további rosszindulatú szoftverek fertőzött eszközökön való telepítésére, kriptovaluta-lopásra és kémkedési kampányokra használnak. A LummaC2 rosszindulatú szoftver használatával elkövetett kibertámadásokat többek között olyan pénzügyi indíttatású, kiberfenyegetés mögött álló szereplők is használják, mint a Storm-113, a Storm-1607, a Storm-1674 és az Octo Tempest. A LummaC2 rosszindulatú szoftvert felhasználják a tagállamok alapvető társadalmi és gazdasági tevékenységeinek fenntartásához szükséges kritikus állami funkciók és szolgáltatások elleni kibertámadásokhoz. 2024-ben és 2025-ben a LummaC2 világszerte az információk ellopására leggyakrabban használt eszközök egyike volt. Ezért Maksim Gordienko a LummaC2 fejlesztőjeként, forgalmazójaként és értékesítőjeként olyan, jelentős hatású kibertámadásokban vesz részt – és segíti elő azokat –, amelyek külső fenyegetést jelentenek a tagállamok számára.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Születési idő: 1980.1.25. Születési hely: USSR Állampolgárság: orosz Nem: férfi Kapcsolódó személyek: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Kapcsolódó szervezetek: a GRU 29155. számú egysége (GRU Unit 29155), »Impuls« LLC	Evgeniy Bashev a GRU orosz katonai hírszerző ügynökség 29155. számú egységének (GRU Unit 29155) tagja. Az egységen belül támogatja és elősegíti a tagállamok ellen irányuló, jelentős hatású kibertámadásokat, többek között a feltöréses műveletekhez használt »Aegon« szerver ellenőrzése révén. Mindenekelőtt technikai és anyagi támogatást nyújt a GRU 29155. számú egysége által végrehajtott kibertámadásokhoz az »Impuls« LLC nevű vállalatán keresztül, amely elősegítette az operatív fedezés, az infrastruktúra és a kifizetések biztosítását, valamint kezelte a kibertámadásokhoz használt technikai eszközöket, többek között szervereket. Evgeniy Bashev ezenkívül a GRU struktúrái és a külső hekkerhálózatok közötti együttműködést is koordinálta. Az általa elősegített kibertámadások az alapvető társadalmi és/vagy gazdasági tevékenységek fenntartásához szükséges kritikus állami funkciókat, rendszereket és szolgáltatásokat vették célba a tagállamokban, különösen a közlekedési ágazatban. A GRU 29155. számú egysége a WhisperGate kampány révén Ukrajna kritikus infrastruktúráját is célba vette. Evgeniy Bashev tehát technikai és anyagi támogatást nyújt a tagállamok számára külső fenyegetést jelentő, jelentős hatású kibertámadásokhoz – ideértve a potenciálisan jelentős hatású kibertámadási kísérleteket –, valamint harmadik ország elleni, jelentős hatású kibertámadásokhoz, illetve egyéb módon részt vesz azokban. Kapcsolatban áll az »Impuls« LLC nevű vállalattal mint annak tulajdonosa és vezérigazgatója. Kapcsolatban áll a GRU 29155. számú egységével is mint annak tagja.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Születési hely: Russian Federation Állampolgárság: orosz Nem: férfi Kapcsolódó személyek: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Kapcsolódó szervezetek: a GRU 29155. számú egysége (GRU Unit 29155)	Roman Puntus az orosz katonai hírszerző ügynökség (GRU) 29155. számú egységének (GRU Unit 29155) tagja. Az egységen belül vezető szerepet tölt be a tagállamok elleni jelentős hatású kibertámadások megszervezésében és koordinálásában. Emellett támogatja az egység belső kiberképességeinek fejlesztését, ideértve a személyzet – például hekkerek és programozók – toborzását és felügyeletét. Az »Aegeon-Impuls« nevű fedőcég létrehozásával segítette a kiberműveletek logisztikai és pénzügyi vonatkozásait. Az egység az ő koordináló tevékenysége mellett az alapvető társadalmi vagy gazdasági tevékenységek fenntartásához szükséges kritikus állami funkciókat, rendszereket és szolgáltatásokat célzó kibertámadásokat hajtott végre a tagállamokban, különösen a közlekedési ágazatban. A GRU 29155. számú egysége a WhisperGate kampány révén Ukrajna kritikus infrastruktúráját is célba vette. Roman Puntust ezért felelősség terheli a tagállamok számára külső fenyegetést jelentő, jelentős hatású kibertámadásokért – ideértve a potenciálisan jelentős hatású kibertámadási kísérleteket –, valamint harmadik ország elleni, jelentős hatású kibertámadásokért, illetve egyéb módon részt vesz azokban. Kapcsolatban áll a GRU 29155. számú egységével is mint annak tagja.	2026.7.13.”.

2. A „B. Jogi személyek, szervezetek vagy szervek” cím alatt a szöveg a következő bejegyzésekkel egészül ki:

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
„8.	Media Land LLC	Cím: Tsvetnochnaya st., 16 Litera P, Room 27; Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation A szervezet típusa: korlátolt felelősségű társaság A bejegyzés helye: St Petersburg A bejegyzés dátuma: 2015.10.19. Cégjegyzékszám: 1152536009900 Az üzleti tevékenység fő helye: St Petersburg, Russian Federation Kapcsolódó szervezet: ML.Cloud	2016 óta a Bullet Proof Hosting Service Media Land LLC rosszindulatú szoftverrel elkövetett támadások széles körét segíti elő a tagállamok ellen és világszerte, azáltal, hogy olyan tárhelyszolgáltatásokat kínál, amelyek segítségével elrejtik a felhasználói azonosítókat és kivédik tartalmaknak a bűnüldöző szervek általi eltávolítását, jelentős pénzügyi veszteségeket okozva. A Media Land LLC olyan nagyszabású zsarolóvírus-műveleteket, irányítási és vezérlési szolgáltatásokat, valamint adathalászatra irányuló műveleteket tett lehetővé, amelyek kritikus infrastruktúrákat és alapvető szolgáltatásokat vesznek célba a tagállamokban. A Media Land LLC által elősegített műveletek közé tartozik többek között a LockBit, az EvilCorp és a BlackBasta. A Media Land LLC tehát olyan, jelentős hatású kibertámadásokban vesz részt, amelyek külső fenyegetést jelentenek a tagállamok számára.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
9.	ML.Cloud	Cím: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 A bejegyzés helye: Riga Kapcsolódó személy: Alexander Volosovik Egyéb kapcsolódó szervezetek: Media Land LLC	Az ML.Cloud a Media Land LLC testvérvállalata, és a technikai infrastruktúrát biztosítja a Media Land LLC számára. 2016 óta a Bullet Proof Hosting Service Media Land LLC rosszindulatú szoftverrel elkövetett támadások széles körét segíti elő a tagállamok ellen és világszerte, azáltal, hogy olyan tárhelyszolgáltatásokat kínál, amelyek segítségével elrejtik a felhasználói azonosítókat és kivédik tartalmaknak a bűnüldöző szervek általi eltávolítását, jelentős pénzügyi veszteségeket okozva. A Media Land LLC olyan nagyszabású zsarolóvírus-műveleteket, irányítási és vezérlési szolgáltatásokat, valamint adathalászatra irányuló műveleteket tett lehetővé, amelyek kritikus infrastruktúrákat és alapvető szolgáltatásokat vesznek célba a tagállamokban. A Media Land LLC által elősegített műveletek közé tartozik többek között a LockBit, az EvilCorp és a BlackBasta. A Media Land LLC tehát olyan, jelentős hatású kibertámadásokban vesz részt, amelyek külső fenyegetést jelentenek a tagállamok számára. A ML.Cloud tehát olyan, jelentős hatású kibertámadásokhoz nyújt technikai támogatást, amelyek külső fenyegetést jelentenek a tagállamok számára.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
10.	»Impuls« LLC	Общество с ограниченной ответственностью »Импульс« Cím: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 A szervezet típusa: korlátolt felelősségű társaság A bejegyzés helye: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation A bejegyzés dátuma: 2010.9.27. Cégjegyzékszám: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Az üzleti tevékenység fő helye: Russian Federation Kapcsolódó személyek: Evgeniy Bashev Kapcsolódó szervezetek: a GRU 29155. számú egysége (GRU Unit 29155)	Az »Impuls« LLC orosz vállalat, amelynek tulajdonosa Evgeniy Viktorovich Bashev, a GRU orosz katonai hírszerző ügynökség 29155. számú egységének (GRU Unit 29155) tagja. A vállalat technikai és anyagi támogatást nyújt a GRU 29155. számú egysége által végrehajtott kibertámadásokhoz és kibertámadási kísérletekhez. Az »Impuls« LLC mindenekelőtt operatív közvetítőként játszik szerepet, lehetővé téve, hogy a feltöréses műveletekkel kapcsolatos tevékenységeket egy olyan vállalaton keresztül végezzék, amely hivatalosan nem kapcsolódik az orosz államhoz. Elősegítette az operatív fedezés, az infrastruktúra és a kifizetések biztosítását a kibertámadásokhoz, valamint technikai eszközökkel – többek között a hekkertevékenységek támogatására használt szerverekkel – hozható kapcsolatba. Az »Impuls« LLC mindenekelőtt lehetővé tette a GRU struktúrái és a külső hekkerhálózatok közötti együttműködést. Az »Impuls« LLC által elősegített kiberműveletek az alapvető társadalmi és gazdasági tevékenységek fenntartásához szükséges kritikus állami funkciókat és szolgáltatásokat vesznek célba a tagállamokban, különösen a közlekedési ágazatban. A GRU 29155. számú egysége a WhisperGate kampány révén Ukrajna kritikus infrastruktúráját is célba vette. Az »Impuls« LLC tehát technikai és anyagi támogatást nyújt jelentős hatású, a tagállamok számára külső fenyegetést jelentő kibertámadásokhoz, valamint harmadik ország elleni, jelentős hatású kibertámadásokhoz, illetve egyéb módon részt vesz azokban.	2026.7.13.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
11.	Z-Pentest	más néven: »Z-Pentest Alliance«, »Z-Alliance« Az üzleti tevékenység fő helye: Russian Federation Kapcsolódó személyek: Yuliya Pankratova Kapcsolódó szervezetek: Cyber Army of Russia Reborn/CARR X.com-fiók: ZPentest (Fiók felfüggesztve) Telegram-fiók: Zpentestalliance	A Z-pentest oroszbarát haktivista csoport, amely a CARR (Cyber Army of Russia Reborn) és a NoName057 tagjaiból áll, és világszerte kritikus infrastruktúrákat céloz meg, különösen az energia- és a vízügyi ágazatban. A csoport 2024 decemberében egy dán víziközmű-társaság ellen hajtott végre támadást. A Z-pentestet ezért felelősség terheli jelentős hatású, a tagállamok számára külső fenyegetést jelentő kibertámadásokért.	2026.7.13.”.