2026/1714

13.7.2026

REGOLAMENT TA' IMPLIMENTAZZJONI TAL-KUNSILL (UE) 2026/1714

tat-13 ta' Lulju 2026

li jimplimenta r-Regolament (UE) 2019/796 dwar miżuri restrittivi kontra attakki ċibernetiċi li jheddu l-Unjoni jew l-Istati Membri tagħha

IL-KUNSILL TAL-UNJONI EWROPEA,

Wara li kkunsidra t-Trattat dwar il-Funzjonament tal-Unjoni Ewropea,

Wara li kkunsidra r-Regolament tal-Kunsill (UE) 2019/796 tas-17 ta' Mejju 2019 dwar miżuri restrittivi kontra attakki ċibernetiċi li jheddu l-Unjoni jew l-Istati Membri tagħha [1], u b'mod partikolari l-Artikolu 13(1) tiegħu,

Wara li kkunsidra l-proposta tar-Rappreżentant Għoli tal-Unjoni għall-Affarijiet Barranin u l-Politika ta' Sigurtà,

Billi:

(1) Fis-17 ta' Mejju 2019, il-Kunsill adotta r-Regolament (UE) 2019/796.

(2) Bħala parti mill-azzjoni sostnuta, imfassla u koordinata tal-Unjoni kontra awturi persistenti ta' theddid ċibernetiku, jenħtieġ li tmien persuni fiżiċi u erba' entitajiet jiżdiedu mal-lista tal-persuni fiżiċi u ġuridiċi, entitajiet u korpi soġġetti għal miżuri restrittivi li tinsab fl-Anness I tar-Regolament (UE) 2019/796. Dawk il-persuni u entitajiet huma responsabbli għal attakki ċibernetiċi b'effett sinifikanti jew involuti fihom li jikkostitwixxu theddida esterna għall-Unjoni jew għall-Istati Membri tagħha.

(3) Għalhekk, jenħtieġ li l-Anness I tar-Regolament (UE) 2019/796 jiġi emendat skont dan,

ADOTTA DAN IR-REGOLAMENT:

Artikolu 1

L-Anness I tar-Regolament (UE) 2019/796 huwa emendat skont l-Anness ta' dan ir-Regolament.

Artikolu 2

Dan ir-Regolament għandu jidħol fis-seħħ fid-data tal-pubblikazzjoni tiegħu f'*Il-Ġurnal Uffiċjali tal-Unjoni Ewropea*.

Dan ir-Regolament għandu jorbot fl-intier tiegħu u japplika direttament fl-Istati Membri kollha.

Magħmul fi Brussell, it-13 ta' Lulju 2026.

Għall-Kunsill

Il-President

K. KALLAS

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

ANNESS

L-Anness I tar-Regolament (UE) 2019/796 huwa emendat kif ġej:

(1) l-entrati li ġejjin jiżdiedu taħt l-intestatura “A. Persuni fiżiċi”:

	Isem	Informazzjoni ta’ identifikazzjoni	Raġunijiet	Data tal-elenkar
“20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Psewdonimi: ‘Bentley’, ‘Bergen’, ‘Alex Konor’, ‘Benny’, ‘Ben’, ‘Stern’ Data tat-twelid: 23.6.1988 Indirizz: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Nazzjonalità: Russa Sess: raġel Entitajiet assoċjati: TrickBot, Wizard Spider, Conti	Vitaly Kovalev huwa figura għolja fil-programmi tal-malware ‘Trickbot’ u ‘Conti’. Huwa magħruf ukoll bil-laqmijiet online ‘Bentley’, ‘Bergen’, ‘Alex Konor’, ‘Benny’, ‘Ben’ u ‘Stern’. Conti u Trickbot oriġinarjament inħolqu u ġew żviluppati minn Wizard Spider. Wizard Spider wettaq kampanji ta’ ransomware f’setturi differenti, inkluż servizzi essenzjali bħas-saħħa u l-banek, infetta kompjuters madwar id-dinja u l-malware tiegħu ġie żviluppat f’sett ta’ malware modulari ħafna. Il-kampanji minn Wizard Spider, bl-użu ta’ malware bħal Conti u TrickBot, huma responsabbli għal dannu ekonomiku sostanzjali fl-Unjoni Ewropea. Għalhekk, Vitaly Kovalev huwa responsabbli għal attakki ċibernetiċi, u involut fihom, b’effett sinifikanti li jikkostitwixxu theddida esterna għall-Unjoni jew għall-Istati Membri tagħha.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Data tat-twelid: 30.1.1983 Post tat-twelid: USSR Nazzjonalità: Russa Numru tal-passaport: 762988138 Sess: raġel Entitajiet assoċjati: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik huwa s-sid ta' Media Land LLC. Mill-2016, is-servizz ta' Bullet Proof Hosting - Media Land LLC - kien qed jiffaċilita firxa wiesgħa ta' attakki ta' malware kemm kontra l-Unjoni kif ukoll fuq livell dinji, billi offra servizzi ta' hosting li jaħbu l-identitajiet tal-utenti u jirreżistu t-tneħħija mill-infurzar tal-liġi. Media Land LLC ippermettiet operazzjonijiet ta' ransomware fuq skala kbira, servizzi ta' kmand u kontroll, u operazzjonijiet ta' phishing immirati lejn infrastruttura kritika u servizzi essenzjali fl-Istati Membri , li wasslu għal telf finanzjarju sinifikanti. L-operazzjonijiet iffaċilitati minn Media Land LLC jinkludu, fost oħrajn, LockBit, EvilCorp u BlackBasta. Għalhekk, Media Land LLC hija involuta f'attakki ċibernetiċi b'effett sinifikanti li jikkostitwixxu theddida esterna għall-Unjoni jew għall-Istati Membri tagħha. Bħala sid ta' Media Land LLC, Alexander Volosovik huwa responsabbli għal dawn l-attakki ċibernetiċi u huwa involut fihom. Huwa assoċjat ukoll ma' Media Land LLC.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Psewdonimu: 'Dena' Data tat-twelid: 9.10.1989 Post tat-twelid: USSR Nazzjonalità: Russa Sess: raġel Indirizz: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko magħruf ukoll bħala Dena huwa hacker Russu għal CARR (Cyber Army of Russia Reborn). CARR kienet responsabbli għal attakki ċibernetiċi kontra s-servizzi meħtieġa għaż-żamma ta' attivitajiet ekonomiċi essenzjali u funzjonijiet kritiċi tal-istat fl-Istati Membri, kif ukoll kontra infrastruttura fl-Ukrajna u f'pajjiżi terzi oħra. CARR hija marbuta maċ-Ċentru Ewlieni għat-Teknoloġiji Speċjali (GTsST) fid-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GRU). Il-GTsST jibqa' attiv fit-twettiq ta' attakki ċibernetiċi kontra l-Unjoni jew l-Istati Membri tagħha. Il-miri ta' CARR jinkludu l-aġenziji tal-gvern, l-istituzzjonijiet finanzjarji, l-organi tax-xandir, u l-infrastruttura kritika fl-Istati Membri u fl-Istati Uniti. CARR wettqet attakki distribwiti li jwaqqfu s-servizz (DDoS) fl-Ukrajna u kontra gvernijiet u kumpaniji li jinsabu f'pajjiżi li appoġġaw lill-Ukrajna. Għalhekk, Denis Degtyarenko, hacker ewlieni għal CARR, huwa involut f'attakki ċibernetiċi b'effett sinifikanti, inkluż tentattivi ta' attakki ċibernetiċi b'effett potenzjalment sinifikanti, li jikkostitwixxu theddida esterna għall-Istati Membri, kif ukoll kontra stati terzi. Bħala membru ta' CARR, huwa assoċjat ukoll mal-GTsST.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Psewdonimu: 'YUliYA' Data tat-twelid: 6.4.1984 Post tat-twelid: USSR Nazzjonalità: Russa Sess: mara Indirizz: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova hija hacker Russa li ilha taħdem għal CARR (Cyber Army of Russia Reborn) u waqqfet, u tkompli taħdem għal Z-Pentest. CARR kienet responsabbli għal attakki ċibernetiċi kontra s-servizzi meħtieġa għaż-żamma ta' attivitajiet ekonomiċi essenzjali u funzjonijiet kritiċi tal-istat fl-Istati Membri, kif ukoll kontra infrastruttura fl-Ukrajna u f'pajjiżi terzi oħra. CARR hija marbuta maċ-Ċentru Ewlieni għat-Teknoloġiji Speċjali (GTsST) fid-Direttorat Ewlieni tal-Istat Maġġur tal-Forzi Armati tal-Federazzjoni Russa (GRU). Il-GTsST jibqa' attiv fit-twettiq ta' attakki ċibernetiċi kontra l-Unjoni jew l-Istati Membri tagħha. Il-miri ta' CARR jinkludu l-aġenziji tal-gvern, l-istituzzjonijiet finanzjarji, l-organi tax-xandir, u l-infrastruttura kritika fl-Istati Membri u fl-Istati Uniti. CARR wettqet attakki distribwiti li jwaqqfu s-servizz (DDoS) fl-Ukrajna u kontra gvernijiet u kumpaniji li jinsabu f'pajjiżi li appoġġaw lill-Ukrajna. Z-Pentest huwa responsabbli għal attakki ċibernetiċi b'effett sinifikanti kontra, fost l-oħrajn, is-servizzi meħtieġa għaż-żamma ta' attivitajiet essenzjali fl-Istati Membri. Għalhekk, Yuliya Pankratova, hacker ewlenija għal CARR u għal Z-Pentest, hija involuta f'attakki ċibernetiċi b'effett sinifikanti, inkluż tentattivi ta' attakki ċibernetiċi b'effett potenzjalment sinifikanti, li jikkostitwixxu theddida esterna għall-Istati Membri , kif ukoll kontra stati terzi. Hija assoċjata wkoll ma' Z-Pentest.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Psewdonimu: 'Daugn0' Nazzjonalità: allegatament Russa Sess: raġel	Maksim Voronin magħruf ukoll bħala Daugn0 huwa involut fl-iżvilupp, id-distribuzzjoni u l-bejgħ tal-malware li jisraq l-informazzjoni LummaC2 (magħruf ukoll bħala Lumma Infostealer, Lumma Stealer). LummaC2 hija pjattaforma Malware bħala Servizz (Malware-as-a-Service - MaaS), użata biex tisraq data sensittiva, kredenzjali tal-brawżer, kartieri tal-kriptoassi, jew informazzjoni dwar is-sistema, biex tapplika malware addizzjonali fuq apparati infettati, għal serq tal-kriptovaluti u għal kampanji ta' spjunaġġ. L-attakki ċibernetiċi li jinvolvu l-malware LummaC2 jintużaw ukoll minn awturi ta' theddid ċibernetiku motivati finanzjarjament bħal Storm-113, Storm-1607, Storm-1674, Octo Tempest u oħrajn. Il-malware LummaC2 intuża għal attakki ċibernetiċi kontra funzjonijiet u servizzi kritiċi tal-istat meħtieġa għaż-żamma ta' attivitajiet soċjali u ekonomiċi essenzjali tal-Istati Membri. Fl-2024 u l-2025, LummaC2 kien waħda mill-aktar għodod użati għas-serq tal-informazzjoni madwar id-dinja. Għalhekk, Maksim Voronin bħala żviluppatur, distributur u bejjiegħ ta' LummaC2 huwa involut f'attakki ċibernetiċi b'effett sinifikanti, u jiffaċilitahom, li jikkostitwixxu theddida esterna għall-Istati Membri.	13.7.2026

ELI: http://data.europa.eu/eli/reg_impl/2026/1714/oj

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
25.	Maksim Aleksandrovich GORDIENKO magħruf ukoll bħala Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Psewdonimu: 'Lummaseller' Nazzjonalità: allegatament Russa Sess: raġel	Maksim Gordienko magħruf ukoll bħala Lummaseller huwa involut fl-iżvilupp u d-distribuzzjoni tal-malware li jisraq l-informazzjoni LummaC2 (magħruf ukoll bħala Lumma Infostealer, Lumma Stealer). LummaC2 hija pjattaforma Malware bħala Servizz (Malware-as-a-Service - MaaS), użata biex tisraq data sensittiva, kredenzjali tal-brawżer, kartieri tal-kriptoassi, jew informazzjoni dwar is-sistema, biex tapplika malware addizzjonali fuq apparati infettati, għal serq tal-kriptovaluti u għal kampanji ta' spjunaġġ. L-attakki ċibernetiċi li jinvolvu l-malware LummaC2 jintużaw ukoll minn awturi ta' theddid ċibernetiku motivati finanzjarjament bħal Storm-113, Storm-1607, Storm-1674, Octo Tempest u oħrajn. Il-malware LummaC2 intuża għal attakki ċibernetiċi kontra funzjonijiet u servizzi kritiċi tal-istat meħtieġa għaż-żamma ta' attivitajiet soċjali u ekonomiċi essenzjali tal-Istati Membri. Fl-2024 u l-2025 LummaC2 kien waħda mill-aktar għodod użati għas-serq tal-informazzjoni madwar id-dinja. Għalhekk, Maksim Gordienko bħala żviluppatur, distributur u bejjiegħ ta' LummaC2 huwa involut f'attakki ċibernetiċi b'effett sinifikanti, u jiffaċilitahom, li jikkostitwixxu theddida esterna għall-Istati Membri.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Data tat-twelid: 25.1.1980 Post tat-twelid: USSR Nazzjonalità: Russa Sess: raġel Individwi assoċjati: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Entitajiet assoċjati: GRU Unit 29155, 'Impuls' LLC	Evgeniy Bashev huwa membru tal-Aġenzija tal-Intelligence Militari Russa GRU Unit 29155. Fi ħdan l-unità huwa jappoġġa u jiffaċilita l-attakki ċibernetiċi b'effett sinifikanti kontra l-Istati Membri, fost l-oħrajn permezz tal-kontroll tas-server 'Aegon', użat għall-operazzjonijiet ta' hacking. B'mod partikolari, huwa jipprovdi appoġġ tekniku u materjali għall-attakki ċibernetiċi tal-GRU Unit 29155 permezz tal-kumpanija tiegħu 'Impuls' LLC li ffaċilitat il-kopertura operazzjonali, l-infrastruttura, u l-pagamenti, u mmaniġġat assi tekniċi, inkluż servers, li jintużaw għall-attakki ċibernetiċi. Huwa kkoordina wkoll il-kooperazzjoni bejn l-istrutturi tal-GRU u n-networks esterni tal-hackers. L-attakki ċibernetiċi ffaċilitati minnu kienu mmirati lejn sistemi u servizzi kritiċi tal-funzjonijiet tal-istat meħtieġa għaż-żamma ta' attivitajiet soċjali jew ekonomiċi essenzjali fl-Istati Membri, b'mod partikolari fis-settur tat-trasport. Permezz tal-kampanja WhisperGate, il-GRU Unit 29155 mmirat ukoll lejn l-infrastruttura kritika tal-Ukrajna. Għalhekk, Evgeniy Bashev jipprovdi appoġġ tekniku u materjali għal, jew huwa involut b'xi mod ieħor f'attakki ċibernetiċi b'effett sinifikanti, inkluż tentattivi ta' attakki ċibernetiċi b'effett potenzjalment sinifikanti, li jikkostitwixxu theddida esterna għall-Istati Membri, kif ukoll attakki ċibernetiċi b'effett sinifikanti kontra pajjiż terz. Bħala sid u Direttur Ġenerali, huwa assoċjat mal-kumpanija 'Impuls' LLD. Bħala membru tal-GRU Unit 29155, huwa wkoll assoċjat ma' din l-entità.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Post tat-twelid: Russian Federation Nazzjonalità: Russa Sess: raġel Individwi assoċjati: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Entitajiet assoċjati: GRU Unit 29155	Roman Puntus huwa membru tal-Aġenzija tal-Intelligence Militari Russa GRU Unit 29155. Fi ħdan l-unità, huwa għandu rwol ewlieni fl-organizzazzjoni u l-koordinazzjoni ta' attakki ċibernetiċi b'effett sinifikanti kontra l-Istati Membri. Huwa jappoġġa wkoll l-iżvilupp tal-kapaċità ċibernetika interna tal-unità, inkluż ir-reklutaġġ u s-superviżjoni ta' persunal bħal hackers u programmaturi. Billi stabbilixxa l-kumpanija fittizja 'Aegeon-Impulse', huwa ffaċilita l-aspetti loġistiċi u finanzjarji tal-operazzjonijiet ċibernetiċi. Taħt il-koordinazzjoni tiegħu, l-unità wettqet attakki ċibernetiċi mmirati lejn sistemi u servizzi kritiċi tal-funzjonijiet tal-istat meħtieġa għaż-żamma ta' attivitajiet soċjali jew ekonomiċi essenzjali fl-Istati Membri, b'mod partikolari fis-settur tat-trasport. Permezz tal-kampanja WhisperGate, il-GRU Unit 29155 mmirat ukoll lejn l-infrastruttura kritika tal-Ukrajna. Għalhekk, Roman Puntus huwa responsabbli għal, jew huwa involut b'xi mod ieħor f'attakki ċibernetiċi b'effett sinifikanti, inkluż tentattivi ta' attakki ċibernetiċi b'effett potenzjalment sinifikanti, li jikkostitwixxu theddida esterna għall-Istati Membri, kif ukoll attakki ċibernetiċi b'effett sinifikanti kontra pajjiż terz. Bħala membru tal-GRU Unit 29155, huwa wkoll assoċjat ma' din l-entità.	13.7.2026";

(2) L-entrati li ġejjin jiżdiedu taħt l-intestatura “B. Persuni ġuridiċi, entitajiet u korpi”:

	Isem	Informazzjoni ta’ identifikazzjoni	Raġunijiet	Data tal-elenkar
“8.	Media Land LLC	Indirizz: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Tip ta’ entità: Kumpanija b’Responsabbiltà Limitata Post tar-reġistrazzjoni: St Petersburg Data tar-reġistrazzjoni: 19.10.2015 Numru tar-reġistrazzjoni: 1152536009900 Post prinċipali tan-negozju: St Petersburg, Russian Federation Entità assoċjata: ML.Cloud	Mill-2016, is-servizz ta’ Bullet Proof Hosting - Media Land LLC - kien qed jiffaċilita firxa wiesgħa ta’ attakki ta’ malware kontra l-Istati Membri u fuq livell dinji, billi offra servizzi ta’ hosting li jaħbu l-identitajiet tal-utenti u jirreżistu t-tneħħija mill-infurzar tal-liġi, li wassal għal telfiet finanzjarji sinifikanti. Media Land LLC ippermettiet operazzjonijiet ta’ ransomware fuq skala kbira, servizzi ta’ kmand u kontroll, u operazzjonijiet ta’ phishing immirati lejn infrastruttura kritika u servizzi essenzjali fost l-Istati Membri. L-operazzjonijiet iffaċilitati minn Media Land LLC jinkludu, fost oħrajn, LockBit, EvilCorp u BlackBasta. Għalhekk, Media Land LLC hija involuta f’attakki ċibernetiċi b’effett sinifikanti, li jikkostitwixxu theddida esterna għall-Istati Membri.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
9.	ML.Cloud	Indirizz: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Post tar-reġistrazzjoni: Riga Individwu assoċjat: Alexander Volosovik Entitajiet assoċjati oħra: Media Land LLC	ML.Cloud hija l-kumpanija oħt ta' Media Land LLC, u tipprovdi l-infrastruttura teknika għal Media Land LLC. Mill-2016, is-servizz ta' Bullet Proof Hosting - Media Land LLC - kien qed jiffaċilita firxa wiesgħa ta' attakki ta' malware kontra l-Istati Membri u fuq livell dinji, billi offra servizzi ta' hosting li jaħbu l-identitajiet tal-utenti u jirreżistu t-tneħħija mill-infurzar tal-liġi, li wassal għal telfiet finanzjarji sinifikanti. Media Land LLC ippermettiet operazzjonijiet ta' ransomware fuq skala kbira, servizzi ta' kmand u kontroll, u operazzjonijiet ta' phishing immirati lejn infrastruttura kritika u servizzi essenzjali fost l-Istati Membri. L-operazzjonijiet iffaċilitati minn Media Land LLC jinkludu, fost oħrajn, LockBit, EvilCorp u BlackBasta. Għalhekk, Media Land LLC hija involuta f'attakki ċibernetiċi li jikkostitwixxu theddia esterna b'effett sinifikanti lill-Istati Membri tal-UE. Għalhekk, ML. Cloud tipprovdi appoġġ tekniku għal attakki ċibernetiċi b'effett sinifikanti, li jikkostitwixxu theddida esterna għall-Istati Membri.	13.7.2026

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
10.	'Impuls' LLC	Общество с ограниченной ответственностью 'Импульс' Indirizz: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Tip ta' entità: Kumpanija b'Responsabbiltà Limitata Post tar-reġistrazzjoni: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Data tar-reġistrazzjoni: 27.9.2010 Numru tar-reġistrazzjoni: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Post prinċipali tan-negozju: Russian Federation Individwi assoċjati: Evgeniy Bashev Entitajiet assoċjati: GRU Unit 29155	'Impuls' LLC hija kumpanija Russa proprjetà ta' Evgeniy Viktorovich Bashev, membru tal-Aġenzija tal-Intelligence Militari Russa GRU Unit 29155. Il-kumpanija tipprovdi appoġġ tekniku u materjali għal attakki ċibernetiċi u tentattivi ta' attakki ċibernetiċi mwettqa mill-GRU Unit 29155. B'mod partikolari, 'Impuls' LLC isservi bħala intermedjarju operazzjonali li jippermetti li jitwettqu attivitajiet relatati mal-hacking permezz ta' kumpanija formalment mhux konnessa mal-Istat Russu. Din iffaċilitat il-kopertura operazzjonali, l-infrastruttura u l-pagamenti għal attakki ċibernetiċi, u kienet konnessa ma' assi tekniċi, inkluż servers użati b'appoġġ għall-attivitajiet ta' hacking. B'mod partikolari, 'Impuls' LLC ippermettiet il-kooperazzjoni bejn l-istrutturi tal-GRU u n-networks esterni ta' hackers. L-operazzjonijiet ċibernetiċi ffaċilitati minn 'Impuls' LLC jimmiraw lejn funzjonijiet u servizzi kritiċi tal-istat meħtieġa għaż-żamma ta' attivitajiet soċjali u ekonomiċi essenzjali fl-Istati Membri, b'mod partikolari fis-settur tat-trasport. Permezz tal-kampanja WhisperGate, il-GRU Unit 29155 mmirat ukoll lejn l-infrastruttura kritika tal-Ukrajna. Għalhekk, 'Impuls' LLC tipprovdi appoġġ tekniku u materjali għal attakki ċibernetiċi b'effett sinifikanti, jew inkella hija involuta fihom, li jikkostitwixxu theddida esterna għall-Istati Membri, kif ukoll attakki ċibernetiċi b'effett sinifikanti kontra pajjiż terz.	13.7.2026

ELI: http://data.europa.eu/eli/reg_impl/2026/1714/oj

	Isem	Informazzjoni ta' identifikazzjoni	Raġunijiet	Data tal-elenkar
11.	Z-Pentest	Psewdonimi: 'Z-Pentest Alliance', 'Z-Alliance' Post prinċipali tan-negozju: Russian Federation Individwi assoċjati: Yuliya Pankratova Entitajiet assoċjati: Cyber Army of Russia Reborn/CARR Kont X.com: ZPentest (Kont sospiż) Kont Telegram: Zpentestalliance	Z-Pentest huwa grupp hacktivist favur ir-Russja, magħmul minn membri minn CARR (Cyber Army of Russia Reborn) u NoName057, li globalment għandhom fil-mira l-infrastruttura kritika, speċjalment is-settur tal-enerġija u tal-ilma. B'mod partikolari, il-grupp attakka utilità tal-ilma Daniża f'Diċembru 2024. Għalhekk, Z-Pentest huwa responsabbli għal attakki ċibernetiċi b'effett sinifikanti, li jikkostitwixxu theddida esterna għall-Istati Membri.	13.7.2026".