Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2026/1713

13.7.2026

ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2026/1713 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 13ης Ιουλίου 2026

για την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2019/797 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για την Ευρωπαϊκή Ένωση, και ιδίως το άρθρο 29,

Έχοντας υπόψη την πρόταση του Ύπατου Εκπροσώπου της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας,

Εκτιμώντας τα ακόλουθα:

(1) Στις 17 Μαΐου 2019 το Συμβούλιο εξέδωσε την απόφαση (ΚΕΠΠΑ) 2019/797 ([1]).

(2) Στο πλαίσιο της διαρκούς, εξατομικευμένης και συντονισμένης δράσης της Ένωσης κατά των επίμονων παραγόντων κυβερνοαπειλών, οκτώ φυσικά πρόσωπα και τέσσερις οντότητες θα πρέπει να προστεθούν στον κατάλογο του παραρτήματος της απόφασης (ΚΕΠΠΑ) 2019/797, ο οποίος περιέχει φυσικά και νομικά πρόσωπα, οντότητες και φορείς που τελούν υπό περιοριστικά μέτρα. Τα πρόσωπα και οι οντότητες αυτές ευθύνονται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο που αποτελούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της, στηρίζουν ή εμπλέκονται σε τέτοιες κυβερνοεπιθέσεις.

(3) Η απόφαση (ΚΕΠΠΑ) 2019/797 θα πρέπει, συνεπώς, να τροποποιηθεί αναλόγως,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Το παράρτημα της απόφασης (ΚΕΠΠΑ) 2019/797 τροποποιείται σύμφωνα με το παράρτημα της παρούσας απόφασης.

Άρθρο 2

Η παρούσα απόφαση αρχίζει να ισχύει την ημέρα δημοσίευσής της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Βρυξέλλες, 13 Ιουλίου 2026.

Για το Συμβούλιο

Η Πρόεδρος

K. KALLAS

([1]) Απόφαση (ΚΕΠΠΑ) 2019/797 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 129 I της 17.5.2019, σ. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

ΠΑΡΑΡΤΗΜΑ

Το παράρτημα της απόφασης (ΚΕΠΠΑ) 2019/797 τροποποιείται ως εξής:

1. Οι ακόλουθες καταχωρίσεις προστίθενται υπό την επικεφαλίδα «Α. Φυσικά πρόσωπα»:

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
«20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Άλλως: “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben”, “Stern” Ημερομηνία γέννησης: 23.6.1988 Διεύθυνση: Serebristy Bulvar 34 (Serebristyy Bul'var)· krp 1· flt 528· 197341· Αγία Πετρούπολη, Ρωσική Ομοσπονδία Ιθαγένεια: ρωσική Φύλο: άρρεν Συνδεδεμένες οντότητες: TrickBot, Wizard Spider, Conti	Ο Vitaly Kovalev είναι ανώτερο στέλεχος των προγραμμάτων κακόβουλου λογισμικού “Trickbot” και “Conti”. Είναι επίσης γνωστός με τα διαδικτυακά ψευδώνυμα “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben” και “Stern”. Τα προγράμματα Conti και Trickbot δημιουργήθηκαν αρχικά και αναπτύχθηκαν από τη Wizard Spider. Η Wizard Spider έχει διεξαγάγει εκστρατείες λυτρισμικού σε διάφορους τομείς, συμπεριλαμβανομένων βασικών υπηρεσιών, όπως η υγεία και ο τραπεζικός τομέας, έχει προσβάλει υπολογιστές σε όλο τον κόσμο και το κακόβουλο λογισμικό της έχει εξελιχθεί σε μια εξαιρετικά αρθρωτή σουίτα κακόβουλου λογισμικού. Εκστρατείες της Wizard Spider, που χρησιμοποιούν είδη κακόβουλου λογισμικού, όπως Conti και TrickBot, ευθύνονται για σημαντική οικονομική ζημιά στην Ευρωπαϊκή Ένωση. Κατά συνέπεια, ο Vitaly Kovalev ευθύνεται για κυβερνοεπιθέσεις με σημαντικό αντίκτυπο, οι οποίες αποτελούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της και εμπλέκεται σε τέτοιες κυβερνοεπιθέσεις.	13.7.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Ημερομηνία γέννησης: 30.1.1983 Τόπος γέννησης: ΕΣΣΔ Ιθαγένεια: ρωσική Αριθ. διαβατηρίου: 762988138 Φύλο: άρρεν Συνδεδεμένες οντότητες: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Ο Alexander Volosovik είναι ο ιδιοκτήτης της Media Land LLC. Από το 2016 η Bullet Proof Hosting service Media Land LLC διευκολύνει ευρύ φάσμα επιθέσεων κακόβουλου λογισμικού κατά της Ένωσης και παγκοσμίως, προσφέροντας υπηρεσίες φιλοξενίας που αποκρύπτουν την ταυτότητα των χρηστών και αντιστέκονται στην αφαίρεση περιεχομένου από τις αρχές επιβολής του νόμου. Η MEDIA Land LLC κατέστησε δυνατές μεγάλης κλίμακας επιχειρήσεις λυτρισμικού, υπηρεσίες διοίκησης και ελέγχου και επιχειρήσεις ηλεκτρονικού "ψαρέματος" που στοχεύουν κρίσιμες υποδομές και βασικές υπηρεσίες στα κράτη μέλη, με αποτέλεσμα σημαντικές οικονομικές ζημίες. Στις επιχειρήσεις που διευκολύνθηκαν από την Media Land LLC συγκαταλέγονται οι LockBit, EvilCorp και BlackBasta. Κατά συνέπεια, η Media Land LLC εμπλέκεται σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις που συνιστούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της. Ως ιδιοκτήτης της Media Land LLC, ο Alexander Volosovik ευθύνεται για τις κυβερνοεπιθέσεις και εμπλέκεται σε αυτές. Συνδέεται επίσης με την Media Land LLC.	13.7.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Άλλως: “Dena” Ημερομηνία γέννησης: 9.10.1989 Τόπος γέννησης: ΕΣΣΔ Ιθαγένεια: ρωσική Φύλο: άρρεν Διεύθυνση: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Ρωσική Ομοσπονδία	Ο Denis Degtyarenko, άλλως Dena, είναι Ρώσος χάκερ για τον CARR (Cyber Army of Russia Reborn). Ο CARR είναι υπεύθυνος για κυβερνοεπιθέσεις κατά υπηρεσιών αναγκαίων για τη διατήρηση βασικών οικονομικών δραστηριοτήτων και κρίσιμων κρατικών λειτουργιών στα κράτη μέλη, καθώς και κατά υποδομών στην Ουκρανία και σε άλλες τρίτες χώρες. Ο CARR συνδέεται με το Κύριο Κέντρο Ειδικών Τεχνολογιών (GTsST) εντός της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GRU). Το GTsST εξακολουθεί να πραγματοποιεί κυβερνοεπιθέσεις κατά της Ένωσης ή των κρατών μελών της. Στους στόχους του CARR περιλαμβάνονται κυβερνητικοί οργανισμοί, χρηματοπιστωτικά ιδρύματα, μέσα ενημέρωσης και κρίσιμες υποδομές στα κράτη μέλη και στις Ηνωμένες Πολιτείες. Ο CARR έχει πραγματοποιήσει κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) στην Ουκρανία και κατά κυβερνήσεων και εταιρειών που βρίσκονται σε χώρες οι οποίες έχουν στηρίξει την Ουκρανία. Κατά συνέπεια, ο Denis Degtyarenko, βασικός χάκερ για τον CARR, εμπλέκεται σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, συμπεριλαμβανομένων αποπειρών κυβερνοεπιθέσεων με δυνητικά σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη, καθώς και κατά τρίτων κρατών. Ως μέλος του CARR, συνδέεται επίσης με το GTsST.	13.7.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Άλλως: “YUliYA” Ημερομηνία γέννησης: 6.4.1984 Τόπος γέννησης: ΕΣΣΔ Ιθαγένεια: ρωσική Φύλο: θήλυ Διεύθυνση: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Ρωσική Ομοσπονδία	Η Yuliya Pankratova είναι Ρωσίδα χάκερ που εργάζεται για τον CARR (Cyber Army of Russia Reborn) και ίδρυσε και εξακολουθεί να εργάζεται για την ομάδα Z-Pentest. Ο CARR είναι υπεύθυνος για κυβερνοεπιθέσεις κατά υπηρεσιών αναγκαίων για τη διατήρηση βασικών οικονομικών δραστηριοτήτων και κρίσιμων κρατικών λειτουργιών στα κράτη μέλη, καθώς και κατά υποδομών στην Ουκρανία και σε άλλες τρίτες χώρες. Ο CARR συνδέεται με το Κύριο Κέντρο Ειδικών Τεχνολογιών (GTsST) εντός της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GRU). Το GTsST εξακολουθεί να πραγματοποιεί κυβερνοεπιθέσεις κατά της Ένωσης ή των κρατών μελών της. Στους στόχους του CARR περιλαμβάνονται κυβερνητικοί οργανισμοί, χρηματοπιστωτικά ιδρύματα, μέσα ενημέρωσης και κρίσιμες υποδομές στα κράτη μέλη και στις Ηνωμένες Πολιτείες. Ο CARR έχει πραγματοποιήσει κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) στην Ουκρανία και κατά κυβερνήσεων και εταιρειών που βρίσκονται σε χώρες οι οποίες έχουν στηρίξει την Ουκρανία. Η Z-Pentest είναι υπεύθυνη για κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, μεταξύ άλλων, κατά υπηρεσιών που είναι απαραίτητες για τη διατήρηση βασικών δραστηριοτήτων στα κράτη μέλη. Κατά συνέπεια, η Yuliya Pankratova, βασική χάκερ για τον CARR και τη Z-Pentest, εμπλέκεται σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, συμπεριλαμβανομένων αποπειρών κυβερνοεπιθέσεων με δυνητικά σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη, καθώς και κατά τρίτων κρατών. Συνδέεται επίσης με τη Z-Pentest.	13.7.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Άλλως: “Daugn0” Ιθαγένεια: ρωσική (εικαζόμενη) Φύλο: άρρεν	Ο Maksim Voronin, άλλως Daugn0, εμπλέκεται στην ανάπτυξη, διανομή και πώληση του κακόβουλου λογισμικού LummaC2 που υποκλέπτει πληροφορίες (γνωστού και ως Lumma Infostealer, Lumma Stealer). Το LummaC2 είναι μια πλατφόρμα Malware-as-a-Service (MaaS), η οποία χρησιμοποιείται για την κλοπή ευαίσθητων δεδομένων, διαπιστευτηρίων φυλλομετρητή, κρυπτοπορτοφολιών ή πληροφοριών συστήματος, για την ανάπτυξη πρόσθετου κακόβουλου λογισμικού σε μολυσμένες συσκευές, για κλοπή κρυπτονομισμάτων και για εκστρατείες κατασκοπείας. Οι κυβερνοεπιθέσεις με κακόβουλο λογισμικό LummaC2 χρησιμοποιούνται επίσης από παράγοντες κυβερνοαπειλών με οικονομικά κίνητρα, π.χ. Storm-113, Storm-1607, Storm-1674, Octo Tempest κλπ. Το κακόβουλο λογισμικό LummaC2 έχει χρησιμοποιηθεί για κυβερνοεπιθέσεις κατά κρίσιμων κρατικών λειτουργιών και υπηρεσιών που είναι απαραίτητες για τη διατήρηση των βασικών κοινωνικών και οικονομικών δραστηριοτήτων των κρατών μελών. Το 2024 και το 2025 το LummaC2 ήταν ένα από τα πλέον χρησιμοποιούμενα εργαλεία για την υποκλοπή πληροφοριών παγκοσμίως. Κατά συνέπεια, ο Maksim Voronin, ως φορέας ανάπτυξης, διανομής και πώλησης του LummaC2, εμπλέκεται και διευκολύνει κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη.	13.7.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
25.	Maksim Aleksandrovich GORDIENKO Άλλως: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Άλλως: “Lummaseller” Ιθαγένεια: ρωσική (εικαζόμενη) Φύλο: άρρεν	Ο Maksim Gordienko, άλλως Lummaseller, συμμετέχει στην ανάπτυξη και διανομή του κακόβουλου λογισμικού LummaC2 που υποκλέπτει πληροφορίες (γνωστού και ως Lumma Infostealer, Lumma Stealer). Το LummaC2 είναι μια πλατφόρμα Malware-as-a-Service (MaaS), η οποία χρησιμοποιείται για την κλοπή ευαίσθητων δεδομένων, διαπιστευτηρίων φυλλομετρητή, κρυπτοπορτοφολιών ή πληροφοριών συστήματος, για την ανάπτυξη πρόσθετου κακόβουλου λογισμικού σε μολυσμένες συσκευές, για κλοπή κρυπτονομισμάτων και για εκστρατείες κατασκοπείας. Οι κυβερνοεπιθέσεις με κακόβουλο λογισμικό LummaC2 χρησιμοποιούνται επίσης από παράγοντες κυβερνοαπειλών με οικονομικά κίνητρα, π.χ. Storm-113, Storm-1607, Storm-1674, Octo Tempest κλπ. Το κακόβουλο λογισμικό LummaC2 έχει χρησιμοποιηθεί για κυβερνοεπιθέσεις κατά κρίσιμων κρατικών λειτουργιών και υπηρεσιών που είναι απαραίτητες για τη διατήρηση των βασικών κοινωνικών και οικονομικών δραστηριοτήτων των κρατών μελών. Το 2024 και το 2025 το LummaC2 ήταν ένα από τα πλέον χρησιμοποιούμενα εργαλεία για την υποκλοπή πληροφοριών παγκοσμίως. Κατά συνέπεια, ο Maksim Gordienko, ως φορέας ανάπτυξης, διανομής και πώλησης του LummaC2, εμπλέκεται και διευκολύνει κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη.	13.7.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Ημερομηνία γέννησης: 25.1.1980 Τόπος γέννησης: ΕΣΣΔ Ιθαγένεια: ρωσική Φύλο: άρρεν Συνδεδεμένα πρόσωπα: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Συνδεδεμένες οντότητες: GRU Unit 29155, "Impuls" LLC	Ο Evgeniy Bashev είναι μέλος της ρωσικής στρατιωτικής υπηρεσίας πληροφοριών GRU, Unit 29155. Εντός της μονάδας υποστηρίζει και διευκολύνει κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά των κρατών μελών, μεταξύ άλλων μέσω του ελέγχου του εξυπηρετητή "Aegon", ο οποίος χρησιμοποιείται για επιχειρήσεις δικτυοπαραβίασης. Ειδικότερα, παρέχει τεχνική και υλική υποστήριξη στις κυβερνοεπιθέσεις της GRU Unit 29155 μέσω της εταιρείας του "Impuls" LLC, η οποία διευκόλυνε την επιχειρησιακή κάλυψη, τις υποδομές και τις πληρωμές, καθώς και υπό διαχείριση τεχνικά μέσα, συμπεριλαμβανομένων διακομιστών, που χρησιμοποιούνται για τις κυβερνοεπιθέσεις. Συντόνισε επίσης τη συνεργασία μεταξύ των δομών της GRU και των εξωτερικών δικτύων χάκερ. Οι κυβερνοεπιθέσεις τις οποίες διευκόλυνε είχαν ως στόχο βασικά συστήματα και υπηρεσίες κρατικών λειτουργιών που είναι απαραίτητα για τη διατήρηση ουσιαστικών κοινωνικών ή οικονομικών δραστηριοτήτων στα κράτη μέλη, ιδίως στον τομέα των μεταφορών. Μέσω της εκστρατείας WhisperGate, η GRU Unit 29155 στόχευε επίσης κρίσιμες υποδομές της Ουκρανίας. Ως εκ τούτου, ο Evgeniy Bashev παρέχει τεχνική και υλική υποστήριξη ή εμπλέκεται με άλλον τρόπο σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, συμπεριλαμβανομένων και αποπειρών κυβερνοεπιθέσεων με δυνητικά σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη, καθώς και κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτης χώρας. Ως ιδιοκτήτης και γενικός διευθυντής, συνδέεται με την εταιρεία "Impuls" LLC. Ως μέλος της GRU Unit 29155, συνδέεται επίσης με την εν λόγω οντότητα.	13.7.2026

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Τόπος γέννησης: Ρωσική Ομοσπονδία Ιθαγένεια: ρωσική Φύλο: άρρεν Συνδεδεμένα πρόσωπα: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Συνδεδεμένες οντότητες: GRU Unit 29155	Ο Roman Puntus είναι μέλος της ρωσικής στρατιωτικής υπηρεσίας πληροφοριών GRU Unit 29155. Εντός της μονάδας, διαδραματίζει ηγετικό ρόλο στην οργάνωση και τον συντονισμό κυβερνοεπιθέσεων με σημαντικές επιπτώσεις κατά των κρατών μελών. Υποστηρίζει επίσης την ανάπτυξη της εσωτερικής κυβερνοϊκανότητας της μονάδας, συμπεριλαμβανομένων της πρόσληψης και της εποπτείας προσωπικού, όπως χάκερ και προγραμματιστών. Με τη σύσταση της εταιρείας-προπέτασμα “Aegeon-Impulse”, διευκόλυνε τις υλικοτεχνικές και οικονομικές πτυχές των επιχειρήσεων στον κυβερνοχώρο. Υπό τον συντονισμό του, η μονάδα διεξήγαγε κυβερνοεπιθέσεις που είχαν ως στόχο βασικά συστήματα και υπηρεσίες κρατικών λειτουργιών που είναι απαραίτητα για τη διατήρηση ουσιαστικών κοινωνικών ή οικονομικών δραστηριοτήτων στα κράτη μέλη, ιδίως στον τομέα των μεταφορών. Μέσω της εκστρατείας WhisperGate, η GRU Unit 29155 στόχευε επίσης κρίσιμες υποδομές της Ουκρανίας. Ως εκ τούτου, ο Roman Puntus ευθύνεται ή εμπλέκεται με άλλον τρόπο σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, συμπεριλαμβανομένων και αποπειρών κυβερνοεπιθέσεων με δυνητικά σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη, καθώς και κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτης χώρας. Ως μέλος της GRU Unit 29155, συνδέεται επίσης με την εν λόγω οντότητα.	13.7.2026»

2. Οι ακόλουθες καταχωρίσεις προστίθενται κάτω από την επικεφαλίδα «Β. Νομικά πρόσωπα, οντότητες και φορείς»:

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
«8.	Media Land LLC	Διεύθυνση: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Ρωσική Ομοσπονδία Τύπος οντότητας: Εταιρεία Περιορισμένης Ευθύνης Τόπος εγγραφής σε μητρώο: Αγία Πετρούπολη Ημερομηνία εγγραφής σε μητρώο: 19.10.2015 Αριθμός μητρώου: 1152536009900 Κύριος τόπος δραστηριοτήτων: Αγία Πετρούπολη, Ρωσική Ομοσπονδία Συνδεδεμένη οντότητα: ML.Cloud	Από το 2016 η Bullet Proof Hosting service Media Land LLC διευκολύνει ευρύ φάσμα επιθέσεων κακόβουλου λογισμικού κατά των κρατών μελών και παγκοσμίως, προσφέροντας υπηρεσίες φιλοξενίας που αποκρύπτουν την ταυτότητα των χρηστών και αντιστέκονται στην αφαίρεση περιεχομένου από τις αρχές επιβολής του νόμου, με αποτέλεσμα σημαντικές οικονομικές ζημίες. Η MEDIA Land LLC κατέστησε δυνατές μεγάλης κλίμακας επιχειρήσεις λυτρισμικού, υπηρεσίες διοίκησης και ελέγχου και επιχειρήσεις ηλεκτρονικού “ψαρέματος” που στοχεύουν κρίσιμες υποδομές και βασικές υπηρεσίες μεταξύ των κρατών μελών. Στις επιχειρήσεις που διευκολύνθηκαν από την Media Land LLC συγκαταλέγονται οι LockBit, EvilCorp και BlackBasta. Κατά συνέπεια, η Media Land LLC εμπλέκεται σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη.	13.7.2026

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
9.	ML.Cloud	Διεύθυνση: Brivibas iela 52, Riga, LV-1011, Latvija· Ρωσική Ομοσπονδία, Kazan, Peterburgskaya st. 52 Τόπος εγγραφής σε μητρώο: Ρίγα Συνδεδεμένο πρόσωπο: Alexander Volosovik Άλλες συνδεδεμένες οντότητες: Media Land LLC	Η ML.Cloud είναι η αδελφή εταιρεία της Media Land LLC και παρέχει την τεχνική υποδομή για την Media Land LLC. Από το 2016 η Bullet Proof Hosting service Media Land LLC διευκολύνει ευρύ φάσμα επιθέσεων κακόβουλου λογισμικού κατά των κρατών μελών και παγκοσμίως, προσφέροντας υπηρεσίες φιλοξενίας που αποκρύπτουν την ταυτότητα των χρηστών και αντιστέκονται στην αφαίρεση περιεχομένου από τις αρχές επιβολής του νόμου, με αποτέλεσμα σημαντικές οικονομικές ζημίες. Η MEDIA Land LLC κατέστησε δυνατές μεγάλης κλίμακας επιχειρήσεις λυτρισμικού, υπηρεσίες διοίκησης και ελέγχου και επιχειρήσεις ηλεκτρονικού "ψαρέματος" που στοχεύουν κρίσιμες υποδομές και βασικές υπηρεσίες μεταξύ των κρατών μελών. Στις επιχειρήσεις που διευκολύνθηκαν από την Media Land LLC συγκαταλέγονται οι LockBit, EvilCorp και BlackBasta. Ως εκ τούτου, η Media Land LLC εμπλέκεται σε κυβερνοεπιθέσεις, οι οποίες συνιστούν εξωτερική απειλή με σημαντικές επιπτώσεις για τα κράτη μέλη. Κατά συνέπεια, η ML..Cloud παρέχει τεχνική υποστήριξη για κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη .	13.7.2026

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
10.	“Impuls” LLC	Общество с ограниченной ответственностью “Импульс” Διεύθυνση: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Τύπος οντότητας: Εταιρεία Περιορισμένης Ευθύνης Τόπος εγγραφής σε μητρώο: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Ρωσική Ομοσπονδία Ημερομηνία εγγραφής σε μητρώο: 27.9.2010 Αριθμός μητρώου: INN (ИНН): 6168033776· OGRN (ОГРН): 1106194004850 Κύριος τόπος δραστηριοτήτων: Ρωσική Ομοσπονδία Συνδεδεμένα πρόσωπα: Evgeniy Bashev Συνδεδεμένες οντότητες: GRU Unit 29155	Η “Impuls” LLC είναι ρωσική εταιρεία που ανήκει στον Evgeniy Viktorovich Bashev, μέλος της ρωσικής στρατιωτικής υπηρεσίας πληροφοριών GRU Unit 29155. Η εταιρεία παρέχει τεχνική και υλική υποστήριξη σε κυβερνοεπιθέσεις και απόπειρες κυβερνοεπιθέσεων που πραγματοποιεί η GRU Unit 29155. Ειδικότερα, η “Impuls” LLC λειτουργεί ως επιχειρησιακός διαμεσολαβητής που καθιστά δυνατή την εκτέλεση δραστηριοτήτων που σχετίζονται με τη δικτυοπαραβίαση μέσω εταιρείας που δεν συνδέεται επίσημα με το ρωσικό κράτος. Διευκόλυνε την επιχειρησιακή κάλυψη, τις υποδομές και τις πληρωμές για κυβερνοεπιθέσεις και συνδέθηκε με τεχνικά μέσα, συμπεριλαμβανομένων διακομιστών που χρησιμοποιούνται για τη στήριξη δραστηριοτήτων δικτυοπαραβίασης. Ειδικότερα, η “Impuls” LLC κατέστησε δυνατή τη συνεργασία μεταξύ δομών της GRU και εξωτερικών δικτύων χάκερ. Οι επιχειρήσεις στον κυβερνοχώρο που διευκολύνονται από την “Impuls” LLC στοχεύουν βασικές κρατικές λειτουργίες και υπηρεσίες που είναι αναγκαίες για τη διατήρηση ουσιαστικών κοινωνικών και οικονομικών δραστηριοτήτων στα κράτη μέλη, ιδίως στον τομέα των μεταφορών. Μέσω της εκστρατείας WhisperGate, η GRU Unit 29155 στόχευε επίσης κρίσιμες υποδομές της Ουκρανίας. Ως εκ τούτου, η “Impuls” LLC παρέχει τεχνική και υλική υποστήριξη ή εμπλέκεται με άλλον τρόπο σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη, καθώς και κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτης χώρας.	13.7.2026

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
11.	Z-Pentest	Άλλως: “Z-Pentest Alliance”, “Z-Alliance” Κύριος τόπος δραστηριοτήτων: Ρωσική Ομοσπονδία Συνδεδεμένα πρόσωπα: Yuliya Pankratova Συνδεδεμένες οντότητες: Cyber Army of Russia/CARR Λογαριασμός X.com: ZPentest (έχει ανασταλεί η λειτουργία) Λογαριασμός Telegram: Zpentestalliance	Η Z-Pentest είναι μια φιλορωσική ομάδα ακτιβιστών χάκερ, αποτελούμενη από μέλη του CARR (Cyber Army of Russia Reborn) και του NoName057, η οποία στοχεύει σε υποδομές ζωτικής σημασίας ανά τον κόσμο, ιδίως στον τομέα της ενέργειας και των υδάτων. Ειδικότερα, η ομάδα επιτέθηκε σε δανική επιχείρηση ύδρευσης τον Δεκέμβριο του 2024. Ως εκ τούτου, η Z-Pentest ευθύνεται για κυβερνοεπιθέσεις με σημαντικές επιπτώσεις, οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη.	13.7.2026»