Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2026/1078

12.5.2026

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2026/1078 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 11ης Μαΐου 2026

για την εφαρμογή του κανονισμού (ΕΕ) 2019/796 σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2019/796 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της [1], και ιδίως το άρθρο 13,

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 τον κανονισμό (ΕΕ) 2019/796.

(2) Το Συμβούλιο επανεξέτασε τον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων και φορέων στο παράρτημα Ι του κανονισμού (ΕΕ) 2019/796. Με βάση την εν λόγω επανεξέταση, θα πρέπει να επικαιροποιηθούν οι λόγοι για τη συμπερίληψη τεσσάρων προσώπων και μιας οντότητας στον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων και φορέων που υπόκεινται σε περιοριστικά μέτρα.

(3) Συνεπώς, το παράρτημα Ι του κανονισμού (ΕΕ) 2019/796 θα πρέπει να τροποποιηθεί αναλόγως,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Το παράρτημα Ι του κανονισμού (ΕΕ) 2019/796 τροποποιείται σύμφωνα με το παράρτημα του παρόντος κανονισμού.

Άρθρο 2

Ο παρών κανονισμός αρχίζει να ισχύει την επομένη της δημοσίευσής του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 11 Μαΐου 2026.

Για το Συμβούλιο

Η Πρόεδρος

K. KALLAS

[1] ΕΕ L 129 Ι της 17.5.2019, σ. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ΠΑΡΑΡΤΗΜΑ

Το παράρτημα Ι του κανονισμού (ΕΕ) 2019/796 τροποποιείται ως εξής:

1) Υπό τον τίτλο «Α. Φυσικά πρόσωπα», οι καταχωρίσεις 1, 2, 13 και 14 αντικαθίστανται από τις ακόλουθες αντίστοιχες καταχωρίσεις:

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
«1.	GAO Qiang	Ημερομηνία γέννησης: 4 Οκτωβρίου 1983 Τόπος γέννησης: Επαρχία Shandong, Κίνα Διεύθυνση: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Κίνα Ιθαγένεια: κινεζική Φύλο: άρρεν	Ο Gao Qiang συνδέεται με τον παράγοντα-ομπρέλα “APT10” (Advanced Persistent Threat 10) (άλλως “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” και “Potassium”) και έχει εμπλακεί στην “Operation Cloud Hopper”, μια σειρά κυβερνοεπιθέσεων με σημαντικές επιπτώσεις που προήλθαν από χώρες εκτός της Ένωσης και αποτέλεσαν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της, καθώς και κυβερνοεπιθέσεων με σημαντικές επιπτώσεις εις βάρος τρίτων κρατών. Η “Operation Cloud Hopper” είχε ως στόχο συστήματα πληροφοριών πολυεθνικών εταιρειών σε έξι ηπείρους, συμπεριλαμβανομένων εταιρειών που βρίσκονται στην Ένωση, και απέκτησε πρόσβαση άνευ αδείας σε εμπορικώς ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία. Ο Gao Qiang συνδέεται με την υποδομή διοίκησης και ελέγχου του APT10. Επιπλέον, η Huaying Haitai, εταιρεία χρησιμοποιούμενη από την APT10, η οποία καταχωρίστηκε εξαιτίας της παροχής υποστήριξης στην “Operation Cloud Hopper” και της διευκόλυνσης της “Operation Cloud Hopper”, είχε στην απασχόλησή της τον Gao Qiang. Συνδέεται επίσης με τον Zhang Shilong, ο οποίος συνδέεται με την APT10 και έχει επίσης απασχοληθεί στην Huaying Haitai.	30.7.2020

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
2.	ZHANG Shilong	Ημερομηνία γέννησης: 10 Σεπτεμβρίου 1981 Τόπος γέννησης: Κίνα Διεύθυνση: Hedong, Yuyang Road No 121, Tianjin, Κίνα Ιθαγένεια: κινεζική Φύλο: άρρεν	Ο Zhang Shilong συνδέεται με τον παράγοντα-ομπρέλα “APT10” (Advanced Persistent Threat 10) (άλλως “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” και “Potassium”) και έχει εμπλακεί στην “Operation Cloud Hopper”, μια σειρά κυβερνοεπιθέσεων με σημαντικές επιπτώσεις που προήλθαν από χώρες εκτός της Ένωσης και αποτέλεσαν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της, καθώς και κυβερνοεπιθέσεων με σημαντικές επιπτώσεις εις βάρος τρίτων κρατών. Η “Operation Cloud Hopper” είχε ως στόχο συστήματα πληροφοριών πολυεθνικών εταιρειών σε έξι ηπείρους, συμπεριλαμβανομένων εταιρειών που βρίσκονται στην Ένωση, και απέκτησε πρόσβαση άνευ αδείας σε εμπορικώς ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία. Ο Zhang Shilong συνδέεται με τον APT10, μεταξύ άλλων μέσω του κακόβουλου λογισμικού που ανέπτυξε και δοκίμασε σε σχέση με τις κυβερνοεπιθέσεις τις οποίες διεξήγαγε ο APT10. Επιπλέον, η Huaying Haitai, εταιρεία χρησιμοποιούμενη από την APT10, η οποία καταχωρίστηκε εξαιτίας της παροχής υποστήριξης στην “Operation Cloud Hopper” και της διευκόλυνσης της “Operation Cloud Hopper”, είχε στην απασχόλησή της τον Zhang Shilong. Συνδέεται με τον Gao Qiang, ο οποίος συνδέεται με την APT10 και έχει επίσης απασχοληθεί στην Huaying Haitai.	30.7.2020

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Ημερομηνία γέννησης: 20.4.1989 Τόπος γέννησης: Serpukhov, Ρωσική Ομοσπονδία Ιθαγένεια: ρωσική Διεύθυνση: Serpukhov Φύλο: άρρεν	Ο Mikhail Mikhailovich Tsarev συμμετείχε σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη της ΕΕ. Ο Mikhail Mikhailovich Tsarev, γνωστός και με τα διαδικτυακά ψευδώνυμα “Mango”, “Alexander Grachev”, “Super Misha”, “Ivanov Mixail”, “Misha Krutysha” και “Nikita Andreevich Tsarev”, είναι βασικός παράγοντας για την ανάπτυξη των προγραμμάτων κακόβουλου λογισμικού “Conti” και “Trickbot” και εμπλέκεται στην ομάδα απειλών “Wizard Spider” με έδρα τη Ρωσία. Η Wizard Spider εξακολουθεί να εξελίσσεται και να εντείνει τις δραστηριότητές της. Τα προγράμματα κακόβουλου λογισμικού Conti και Trickbot δημιουργήθηκαν 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. Η ομάδα 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 το Conti, το “Ryuk” TrickBot ή το Black Basta, ευθύνονται για σημαντική οικονομική ζημία στην Ευρωπαϊκή Ένωση. Ως εκ τούτου, ο Mikhail Mikhailovich Tsarev εμπλέκεται σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της.	24.6.2024

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Ημερομηνία γέννησης: 19.5.1982 Τόπος γέννησης: Abakan, Ρωσική Ομοσπονδία Ιθαγένεια: ρωσική Φύλο: άρρεν	Ο Maksim Galochkin συμμετείχε σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για τα κράτη μέλη της ΕΕ. Ο Maksim Galochkin είναι επίσης γνωστός με τα διαδικτυακά ψευδώνυμα “Benalen”, “Bentley”, “Volhvb”, “volhvb”, “manuel”, “Max17” και “Crypt”. Ο Galochkin είναι βασικός παράγοντας για την ανάπτυξη των προγραμμάτων κακόβουλου λογισμικού “Conti” και “Trickbot” και εμπλέκεται στην ομάδα απειλών “Wizard Spider” με έδρα τη Ρωσία. Ηγήθηκε μιας ομάδας δοκιμαστών, με αρμοδιότητες για την ανάπτυξη, την εποπτεία και τη διεξαγωγή δοκιμών για το πρόγραμμα κακόβουλου λογισμικού TrickBot, το οποίο δημιουργήθηκε και αναπτύχθηκε από τη Wizard Spider. Η Wizard Spider εξακολουθεί να εξελίσσεται και να εντείνει τις δραστηριότητές της. Η Wizard Spider έχει διεξαγάγει εκστρατείες λυτρισμικού σε διάφορους τομείς, συμπεριλαμβανομένων βασικών υπηρεσιών όπως η υγεία και ο τραπεζικός τομέας. Η ομάδα 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 το Conti, το “Ryuk” TrickBot ή το Black Basta, ευθύνονται για σημαντική οικονομική ζημία στην Ευρωπαϊκή Ένωση. Ως εκ τούτου, ο Maksim Galochkin εμπλέκεται σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της.	24.6.2024».·

2) Υπό τον τίτλο «Β. Νομικά πρόσωπα, οντότητες και φορείς», η καταχώριση 1 αντικαθίσταται από το ακόλουθο κείμενο:

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
«1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Άλλως: Haitai Technology Development Co. Ltd Τόπος εγκατάστασης: Tianjin, Κίνα	Η Huaying Haitai παρείχε οικονομική, τεχνική ή υλική υποστήριξη και διευκόλυνε την "Operation Cloud Hopper", μια σειρά κυβερνοεπιθέσεων με σημαντικές επιπτώσεις που προήλθαν από χώρες εκτός της Ένωσης και αποτέλεσαν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της, καθώς και κυβερνοεπιθέσεων με σημαντικές επιπτώσεις εις βάρος τρίτων κρατών. Η "Operation Cloud Hopper" είχε ως στόχο συστήματα πληροφοριών πολυεθνικών εταιρειών σε έξι ηπείρους, συμπεριλαμβανομένων εταιρειών που βρίσκονται στην Ένωση, και απέκτησε πρόσβαση άνευ αδείας σε εμπορικώς ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία. Ο παράγων που είναι ευρέως γνωστός ως "APT10" ("Advanced Persistent Threat 10") (άλλως "Red Apollo", "CVNX", "Stone Panda", "MenuPass" και "Potassium") διεξήγαγε την "Operation Cloud Hopper". Η Huaying Haitai μπορεί να συνδεθεί με τον APT10. Επίσης, η Huaying Haitai απασχολούσε τον Gao Qiang και τον Zhang Shilong· αμφότεροι έχουν καταχωρισθεί σε σχέση με την "Operation Cloud Hopper". Ως εκ τούτου, η Huaying Haitai συνδέεται επίσης με τον Gao Qiang και τον Zhang Shilong.	30.7.2020».