

Επίσημη Εφημερίδα L 246 της Ευρωπαϊκής Ένωσης



Έκδοση
στην ελληνική γλώσσα

Νομοθεσία

63ο έτος

30 Ιουλίου 2020

Περιεχόμενα

II Μη νομοθετικές πράξεις

ΚΑΝΟΝΙΣΜΟΙ

- ★ Εκτελεστικός κανονισμός (ΕΕ) 2020/1124 του Συμβουλίου, της 30ής Ιουλίου 2020, για την εφαρμογή του κανονισμού (ΕΕ) 2016/1686 για την επιβολή πρόσθετων περιοριστικών μέτρων κατά του ISIL (Da'esh) και της Αλ Κάιντα και κατά φυσικών και νομικών προσώπων, οντοτήτων ή φορέων που συνδέονται μαζί τους 1
- ★ Εκτελεστικός κανονισμός (ΕΕ) 2020/1125 του Συμβουλίου, της 30ής Ιουλίου 2020, 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 4

ΑΠΟΦΑΣΕΙΣ

- ★ Απόφαση (ΚΕΠΠΑ) 2020/1126 του Συμβουλίου, της 30ής Ιουλίου 2020, σχετικά με την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2016/1693 για την επιβολή περιοριστικών μέτρων κατά των ISIL (Da'esh) και Αλ Κάιντα και προσώπων, ομάδων, επιχειρήσεων και οντοτήτων που συνδέονται μαζί τους 10
- ★ Απόφαση (ΚΕΠΠΑ) 2020/1127 του Συμβουλίου, της 30ής Ιουλίου 2020, για την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2019/797 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της 12

EL

Οι πράξεις των οποίων οι τίτλοι έχουν τυπωθεί με λευκά στοιχεία αποτελούν πράξεις τρεχούσης διαχείρισεως που έχουν θεσπισθεί στο πλαίσιο της γεωργικής πολιτικής και είναι γενικά περιορισμένης χρονικής ισχύος.

Οι τίτλοι όλων των υπολοίπων πράξεων έχουν τυπωθεί με μαύρα στοιχεία και επισημαίνονται με αστερίσκο.

II

(Μη νομοθετικές πράξεις)

ΚΑΝΟΝΙΣΜΟΙ

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2020/1124 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 30ής Ιουλίου 2020

για την εφαρμογή του κανονισμού (ΕΕ) 2016/1686 για την επιβολή πρόσθετων περιοριστικών μέτρων κατά του ISIL (Da'esh) και της Αλ Κάιντα και κατά φυσικών και νομικών προσώπων, οντοτήτων ή φορέων που συνδέονται μαζί τους

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2016/1686 του Συμβουλίου, της 20ής Σεπτεμβρίου 2016, για την επιβολή πρόσθετων περιοριστικών μέτρων κατά του ISIL (Da'esh) και της Αλ Κάιντα και κατά φυσικών και νομικών προσώπων, οντοτήτων ή φορέων που συνδέονται μαζί τους ⁽¹⁾ και ιδίως το άρθρο 4 παράγραφος 1,

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

Εκτιμώντας τα ακόλουθα:

- (1) Στις 20 Σεπτεμβρίου 2016 το Συμβούλιο εξέδωσε τον κανονισμό (ΕΕ) 2016/1686.
- (2) Δεδομένης της απειλής που εξακολουθούν να συνιστούν ο ISIL (Da'esh) και η Αλ Κάιντα, καθώς και φυσικά και νομικά πρόσωπα, οντότητες ή φορείς που συνδέονται μαζί τους, θα πρέπει να προστεθεί ένα πρόσωπο στον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων ή φορέων που παρατίθεται στο παράρτημα Ι του κανονισμού (ΕΕ) 2016/1686.
- (3) Ο κανονισμός (ΕΕ) 2016/1686 θα πρέπει, συνεπώς, να τροποποιηθεί αναλόγως,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Το παράρτημα Ι του κανονισμού (ΕΕ) 2016/1686 τροποποιείται σύμφωνα με το παράρτημα του παρόντος κανονισμού.

Άρθρο 2

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

⁽¹⁾ ΕΕ L 255 της 21.9.2016, σ. 1.

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

Βρυξέλλες, 30 Ιουλίου 2020.

Για το Συμβούλιο
Ο Πρόεδρος
M. ROTH

ΠΑΡΑΡΤΗΜΑ

Η ακόλουθη καταχώριση προστίθεται στον κατάλογο του παραρτήματος I του κανονισμού (ΕΕ) 2016/1686:

«6. Bryan D'ANCONA, ημερομηνία γέννησης: 26 Ιανουαρίου 1997, τόπος γέννησης: Νίκαια (Γαλλία), ιθαγένεια: γαλλική.».

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2020/1125 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 30ής Ιουλίου 2020

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 παράγραφος 1,

Έχοντας υπόψη την πρόταση του Υπατού 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) Τα στοχευμένα περιοριστικά μέτρα κατά των κυβερνοεπιθέσεων με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της είναι μεταξύ των μέτρων που περιλαμβάνονται στο πλαίσιο της Ένωσης για κοινή διπλωματική αντίδραση σε κακόβουλες κυβερνοδραστηριότητες (εργαλειοθήκη για την κυβερνοδιπλωματία) και αποτελούν ένα ζωτικής σημασίας μέσο για την αποτροπή και την αντιμετώπιση τέτοιων δραστηριοτήτων. Περιοριστικά μέτρα μπορούν επίσης να επιβληθούν για την αντιμετώπιση κυβερνοεπιθέσεων με σημαντικές επιπτώσεις εις βάρος τρίτων κρατών ή διεθνών οργανισμών, όπου κρίνεται αναγκαίο για την επίτευξη στόχων της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας που ορίζονται στις σχετικές διατάξεις του άρθρου 21 της Συνθήκης για την Ευρωπαϊκή Ένωση.
- (3) Στις 16 Απριλίου 2018, το Συμβούλιο εξέδωσε συμπεράσματα όπου καταδίκασε απερίφραστα την κακόβουλη χρήση τεχνολογιών των πληροφοριών και των επικοινωνιών, μεταξύ άλλων στις κυβερνοεπιθέσεις που έγιναν ευρέως γνωστές με τα ονόματα «WannaCry» και «NotPetya» και οι οποίες προκάλεσαν σοβαρή βλάβη και οικονομική ζημία εντός και εκτός των συνόρων της Ένωσης. Στις 4 Οκτωβρίου 2018, οι Πρόεδροι του Ευρωπαϊκού Συμβουλίου και της Ευρωπαϊκής Επιτροπής και ο Υπάτος Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας («Υπάτος Εκπρόσωπος») εξέφρασαν σοβαρές ανησυχίες σε κοινή δήλωση σχετικά με την απόπειρα κυβερνοεπίθεσης με σκοπό να υπονομευθεί η ακεραιότητα του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες, μια επιθετική ενέργεια που έδειξε περιφρόνηση για τον επίσημο σκοπό του ΟΑΧΟ. Με δήλωση εξ ονόματος της Ένωσης στις 12 Απριλίου 2019, ο Υπάτος Εκπρόσωπος προέτρεψε τους εμπλεκόμενους να σταματήσουν να προβαίνουν σε κακόβουλες κυβερνοδραστηριότητες που αποσκοπούν στην υπονόμηση της ακεραιότητας, της ασφαλείας και της οικονομικής ανταγωνιστικότητας της Ένωσης, συμπεριλαμβανομένων πράξεων κλοπής διανοητικής ιδιοκτησίας μέσω του κυβερνοχώρου. Μεταξύ των εν λόγω κλοπών μέσω του κυβερνοχώρου περιλαμβάνονται εκείνες που πραγματοποιεί ο παράγων ο οποίος είναι ευρέως γνωστός ως «APT10» («Advanced Persistent Threat 10»).
- (4) Στο πλαίσιο αυτό, και με στόχο την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση της συνεχιζόμενης και αυξανόμενης κακόβουλης συμπεριφοράς στον κυβερνοχώρο, θα πρέπει να συμπεριληφθούν έξι φυσικά πρόσωπα και τρεις οντότητες ή φορείς στον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων και φορέων που υπόκεινται σε περιοριστικά μέτρα που παρατίθεται στο παράρτημα Ι του κανονισμού (ΕΕ) 2019/796. Τα εν λόγω πρόσωπα και οντότητες ή φορείς είναι υπεύθυνα για κυβερνοεπιθέσεις ή απόπειρες κυβερνοεπιθέσεων, συμπεριλαμβανομένων της απόπειρας κυβερνοεπίθεσης κατά του ΟΑΧΟ και των κυβερνοεπιθέσεων που έγιναν ευρέως γνωστές με τα ονόματα «WannaCry» και «NotPetya», καθώς και «Operation Cloud Hopper», ή παρείχαν υποστήριξη ή ενεπλόκησαν σε αυτές ή τις διευκόλυναν.
- (5) Ο κανονισμός (ΕΕ) 2019/796 θα πρέπει, συνεπώς, 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.

⁽¹⁾ ΕΕ L 129I της 17.5.2019, σ. 1.

Άρθρο 2

Ο παρών κανονισμός αρχίζει να ισχύει την ημερομηνία 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, 30 Ιουλίου 2020.

Για το Συμβούλιο
Ο Πρόεδρος
M. ROTH

ΠΑΡΑΡΤΗΜΑ

Τα ακόλουθα πρόσωπα και οντότητες ή φορείς προστίθενται στον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων και φορέων που παρατίθεται στο παράρτημα Ι του κανονισμού (ΕΕ) 2019/796:

«Α. Φυσικά πρόσωπα

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
1.	GAO Qiang	<p>Τόπος γέννησης: Επαρχία Shandong, Κίνα Διεύθυνση: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Ίθαγένεια: Κινεζική Φύλο: άρρεν</p>	<p>Ο Gao Qiang εμπλέκεται 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 εμπορικές ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία.</p> <p>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”.</p> <p>Ο Gao Qiang μπορεί να συνδεθεί με τον APT10, μεταξύ άλλων μέσω της σχέσης του με την υποδομή διοίκησης και ελέγχου του APT10. Επιπλέον, η Huaying Haitai, οντότητα που καταχωρίστηκε εξαιτίας της παροχής υποστήριξης και της διευκόλυνσης της “Operation Cloud Hopper”, απασχολούσε τον Gao Qiang. Ο Gao Qiang συνδέεται με τον Zhang Shilong, ο οποίος έχει επίσης καταχωριστεί σε σχέση με την “Operation Cloud Hopper”. Ως εκ τούτου, ο Gao Qiang συνδέεται και με την Huaying Haitai και με τον Zhang Shilong.</p>	30.7.2020
2.	ZHANG Shilong	<p>Διεύθυνση: Hedong, Yuyang Road No 121, Tianjin, China Ίθαγένεια: Κινεζική Φύλο: άρρεν</p>	<p>Ο Zhang Shilong εμπλέκεται 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 εμπορικές ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία.</p> <p>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”.</p> <p>Ο Zhang Shilong μπορεί να συνδεθεί 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, οντότητα που καταχωρίστηκε εξαιτίας της παροχής υποστήριξης και της διευκόλυνσης της “Operation Cloud Hopper”, απασχολούσε τον Zhang Shilong. Συνδέεται με τον Gao Qiang, ο οποίος έχει επίσης καταχωριστεί σε σχέση με την “Operation Cloud Hopper”. Ως εκ τούτου, ο Zhang Shilong συνδέεται και με την Huaying Haitai και με τον Gao Qiang.</p>	30.7.2020

3.	Alexey Valeryevich MININ	<p>Алексей Валерьевич МИНИН Ημερομηνία γέννησης: 27 Μαΐου 1972 Τόπος γέννησης: Περιφέρεια Perm, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 120017582 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς: από 17 Απριλίου 2017 έως 17 Απριλίου 2022 Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία Ιθαγένεια: Ρωσική Φύλο: άρρεν</p>	<p>Ο Alexey Minin συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες. Ως υπεύθυνος υποστήριξης για πληροφορίες από ανθρώπινο υλικό της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Alexey Minin ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδείας στο δίκτυο WiFi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020
4.	Aleksi Sergeevich MORENETS	<p>Алексей Валерьевич МИНИН Ημερομηνία γέννησης: 31 Ιουλίου 1977 Τόπος γέννησης: Περιφέρεια Murmanskaya, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 100135556 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς από: 17 Απριλίου 2017 έως 17 Απριλίου 2022 Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία Ιθαγένεια: Ρωσική Φύλο: άρρεν</p>	<p>Ο Aleksei Morenets συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες. Ως χειριστής κυβερνοχώρου της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Aleksei Morenets ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδείας στο δίκτυο WiFi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	<p>Евгений Михайлович СЕРЕБРЯКОВ Ημερομηνία γέννησης: 26 Ιουλίου 1981 Τόπος γέννησης: Kursk, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 100135555 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς: από 17 Απριλίου 2017 έως 17 Απριλίου 2022 Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία Ιθαγένεια: Ρωσική Φύλο: άρρεν</p>	<p>Ο Evgenii Serebriakov συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες. Ως χειριστής κυβερνοχώρου της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Evgenii Serebriakov ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδείας στο δίκτυο Wi-Fi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020

6.	Oleg Mikhaylovich SOTNIKOV	<p>Олег Михайлович СОТНИКОВ Ημερομηνία γέννησης: 24 Αυγούστου 1972 Τόπος γέννησης: Ulyanovsk, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 120018866 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς από: 17 Απριλίου 2017 έως 17 Απριλίου 2022 Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία Ίθαγένεια: Ρωσική Φύλο: άρρεν</p>	<p>Ο Oleg Sotnikov συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες. Ως υπεύθυνος υποστήριξης για πληροφορίες από ανθρώπινο υλικό της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Oleg Sotnikov ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδείας στο δίκτυο WiFi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020
----	----------------------------	---	--	-----------

B. Νομικά πρόσωπα, οντότητες και φορείς

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	<p>Άλλως: Haitai Technology Development Co. Ltd Τόπος εγκατάστασης: Tianjin, Κίνα</p>	<p>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 εμπορικά 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 καταχωριστεί σε σχέση με την “Operation Cloud Hopper”. Ως εκ τούτου, η Huaying Haitai συνδέεται με τον Gao Qiang και τον Zhang Shilong.</p>	30.7.2020
2.	Chosun Expo	<p>Άλλως: Chosen Expo, Korea Export Joint Venture Τόπος εγκατάστασης: ΛΔΚ</p>	<p>Η Chosun Expo παρείχε οικονομική, τεχνική ή υλική υποστήριξη και διευκόλυνε 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, συμπεριλαμβανομένων των κυβερνοεπιθέσεων που έγιναν ευρέως γνωστές ως “WannaCry” και των κυβερνοεπιθέσεων κατά της Πολωνικής Αρχής Χρηματοπιστωτικής Εποπτείας και της Sony Pictures Entertainment, καθώς και κυβερνοκλοπής από την Bangladesh Bank και απόπειρας κυβερνοκλοπής από τη Vietnam Tien Phong Bank.</p>	30.7.2020

			<p>Η «WannaCry» διατάραξε τη λειτουργία των συστημάτων πληροφοριών σε παγκόσμιο επίπεδο, στοχεύοντας σε συστήματα πληροφοριών με λυτρισμικό και εμποδίζοντας την πρόσβαση σε δεδομένα. Επηρέασε τα συστήματα πληροφοριών εταιρειών στην Ένωση, συμπεριλαμβανομένων των συστημάτων πληροφοριών που σχετίζονται με υπηρεσίες αναγκαίες για τη διατήρηση βασικών υπηρεσιών και οικονομικών δραστηριοτήτων στο εσωτερικό κρατών μελών.</p> <p>Ο παράγων που είναι ευρέως γνωστός ως “APT38” (“Advanced persistent Threat 38”) ή η “Lazarus Group” διεξήγαγε την “WannaCry”.</p> <p>Η Chosun Expro μπορεί να συνδεθεί με τον APT38/τη Lazarus Group, μεταξύ άλλων μέσω των λογαριασμών που χρησιμοποιούνται για τις κυβερνοεπιθέσεις.</p>	
3.	Κύριο Κέντρο Ειδικών Τεχνολογιών (GTsST) της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU)	Διεύθυνση: 22 Kirova Street, Moscow, Russian Federation	<p>Το Κύριο Κέντρο Ειδικών Τεχνολογιών (GTsST) της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), γνωστό και με τον αριθμό αναφοράς 74455, είναι υπεύθυνο για κυβερνοεπιθέσεις με σημαντικές επιπτώσεις που προήλθαν από χώρες εκτός της Ένωσης και αποτέλεσαν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της, καθώς και για κυβερνοεπιθέσεις με σημαντικές επιπτώσεις εις βάρος τρίτων κρατών, συμπεριλαμβανομένων των κυβερνοεπιθέσεων που έγιναν ευρέως γνωστές ως “NotPetya” ή “EternalPetya” του Ιουνίου του 2017 και των κυβερνοεπιθέσεων με στόχο ουκρανικό δίκτυο ηλεκτρικής ενέργειας τον χειμώνα του 2015 και του 2016.</p> <p>Η “NotPetya” ή “EternalPetya” στέρησε από διάφορες εταιρείες στην Ένωση, στην ευρύτερη Ευρώπη και παγκοσμίως την πρόσβαση σε δεδομένα, στοχεύοντας υπολογιστές με λυτρισμικό και εμποδίζοντας την πρόσβαση σε δεδομένα, με αποτέλεσμα, μεταξύ άλλων, σημαντική οικονομική ζημία. Η κυβερνοεπίθεση σε ουκρανικό δίκτυο ηλεκτρικής ενέργειας είχε ως αποτέλεσμα τη διακοπή της λειτουργίας ορισμένων τμημάτων του κατά τη διάρκεια του χειμώνα.</p> <p>Ο παράγων που είναι ευρέως γνωστός ως “Sandworm” (άλλως “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” και “Telebots”), ο οποίος είναι επίσης υπεύθυνος για την επίθεση στο ουκρανικό δίκτυο ηλεκτρικής ενέργειας, διεξήγαγε τη “NotPetya” ή “EternalPetya”.</p> <p>Το Κύριο Κέντρο Ειδικών Τεχνολογιών της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας διαδραματίζει ενεργό ρόλο στις δραστηριότητες στον κυβερνοχώρο που αναλαμβάνει ο Sandworm και μπορεί να συνδεθεί με τον Sandworm.</p>	30.7.2020».

ΑΠΟΦΑΣΕΙΣ

ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2020/1126 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 30ής Ιουλίου 2020

σχετικά με την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2016/1693 για την επιβολή περιοριστικών μέτρων κατά των ISIL (Da'esh) και Αλ Κάιντα και προσώπων, ομάδων, επιχειρήσεων και οντοτήτων που συνδέονται μαζί τους

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

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

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

Εκτιμώντας τα ακόλουθα:

- (1) Στις 20 Σεπτεμβρίου 2016 το Συμβούλιο εξέδωσε την απόφαση (ΚΕΠΠΑ) 2016/1693 ⁽¹⁾ για την επιβολή περιοριστικών μέτρων κατά των ISIL (Da'esh) και Αλ Κάιντα και προσώπων, ομάδων, επιχειρήσεων και οντοτήτων που συνδέονται μαζί τους.
- (2) Δεδομένης της απειλής που εξακολουθούν να συνιστούν οι ISIL (Da'esh) και Αλ Κάιντα και πρόσωπα, ομάδες, επιχειρήσεις και οντότητες που συνδέονται μαζί τους, θα πρέπει να προστεθεί ένα πρόσωπο στον κατάλογο των προσώπων, ομάδων, επιχειρήσεων και οντοτήτων που παρατίθεται στο παράρτημα της απόφασης (ΚΕΠΠΑ) 2016/1693.
- (3) Συνεπώς, η απόφαση (ΚΕΠΠΑ) 2016/1693 θα πρέπει να τροποποιηθεί αναλόγως,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Το παράρτημα της απόφασης (ΚΕΠΠΑ) 2016/1693 τροποποιείται σύμφωνα με το παράρτημα της παρούσας απόφασης.

Άρθρο 2

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

Βρυξέλλες, 30 Ιουλίου 2020.

Για το Συμβούλιο
Ο Πρόεδρος
M. ROTH

⁽¹⁾ Απόφαση (ΚΕΠΠΑ) 2016/1693 του Συμβουλίου, της 20ής Σεπτεμβρίου 2016, για την επιβολή περιοριστικών μέτρων κατά των ISIL (Da'esh) και Αλ Κάιντα και προσώπων, ομάδων, επιχειρήσεων και οντοτήτων που συνδέονται μαζί τους, και για την κατάργηση της κοινής θέσης 2002/402/ΚΕΠΠΑ (ΕΕ L 255 της 21.9.2016, σ. 25).

ΠΑΡΑΡΤΗΜΑ

Η ακόλουθη καταχώριση προστίθεται στον κατάλογο του παραρτήματος της απόφασης (ΚΕΠΠΑ) 2016/1693:

«6. Bryan D'ANCONA, ημερομηνία γέννησης: 26 Ιανουαρίου 1997, τόπος γέννησης: Νίκαια (Γαλλία), ιθαγένεια: γαλλική.».

ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2020/1127 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 30ής Ιουλίου 2020

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) Τα στοχευμένα περιοριστικά μέτρα κατά των κυβερνοεπιθέσεων με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της είναι μεταξύ των μέτρων που περιλαμβάνονται στο πλαίσιο της Ένωσης για κοινή διπλωματική αντίδραση σε κακόβουλες κυβερνοδραστηριότητες (εργαλειοθήκη για την κυβερνοδιπλωματία) και αποτελούν ένα ζωτικής σημασίας μέσο για την αποτροπή και την αντιμετώπιση τέτοιων δραστηριοτήτων. Περιοριστικά μέτρα μπορούν επίσης να επιβληθούν για την αντιμετώπιση κυβερνοεπιθέσεων με σημαντικές επιπτώσεις εις βάρος τρίτων κρατών ή διεθνών οργανισμών, όπου κρίνεται αναγκαίο για την επίτευξη στόχων της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας που ορίζονται στις σχετικές διατάξεις του άρθρου 21 της Συνθήκης για την Ευρωπαϊκή Ένωση.
- (3) Στις 16 Απριλίου 2018, το Συμβούλιο εξέδωσε συμπεράσματα όπου καταδίκασε απερίφραστα την κακόβουλη χρήση τεχνολογιών των πληροφοριών και των επικοινωνιών, μεταξύ άλλων στις κυβερνοεπιθέσεις που έγιναν ευρέως γνωστές με τα ονόματα «WannaCry» και «NotPetya» και οι οποίες προκάλεσαν σοβαρή βλάβη και οικονομική ζημία εντός και εκτός των συνόρων της Ένωσης. Στις 4 Οκτωβρίου 2018, οι Πρόεδροι του Ευρωπαϊκού Συμβουλίου και της Ευρωπαϊκής Επιτροπής και ο ύπατος εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας («ύπατος εκπρόσωπος») εξέφρασαν σοβαρές ανησυχίες σε κοινή δήλωση σχετικά με την απόπειρα κυβερνοεπίθεσης με σκοπό να υπονομευθεί η ακεραιότητα του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες, μια επιθετική ενέργεια που έδειξε περιφρόνηση για τον επίσημο σκοπό του ΟΑΧΟ. Με δήλωση εξ ονόματος της Ένωσης στις 12 Απριλίου 2019, ο ύπατος εκπρόσωπος προέτρεψε τους εμπλεκόμενους να σταματήσουν να προβαίνουν σε κακόβουλες κυβερνοδραστηριότητες που αποσκοπούν στην υπονόμευση της ακεραιότητας, της ασφαλείας και της οικονομικής ανταγωνιστικότητας της Ένωσης, συμπεριλαμβανομένων πράξεων κλοπής διανοητικής ιδιοκτησίας μέσω του κυβερνοχώρου. Μεταξύ των εν λόγω κλοπών μέσω του κυβερνοχώρου περιλαμβάνονται εκείνες που πραγματοποιεί ο παράγων ο οποίος είναι ευρέως γνωστός ως «APT10» («Advanced Persistent Threat 10»).
- (4) Στο πλαίσιο αυτό και με στόχο την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση της συνεχιζόμενης και αυξανόμενης κακόβουλης συμπεριφοράς στον κυβερνοχώρο, θα πρέπει να συμπεριληφθούν έξι φυσικά πρόσωπα και τρεις οντότητες ή φορείς στον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων και φορέων που υπόκεινται σε περιοριστικά μέτρα που παρατίθεται στο παράρτημα της απόφασης (ΚΕΠΠΑ) 2019/797. Τα εν λόγω πρόσωπα και οντότητες ή φορείς είναι υπεύθυνα για κυβερνοεπιθέσεις ή απόπειρες κυβερνοεπιθέσεων, συμπεριλαμβανομένων της απόπειρας κυβερνοεπίθεσης κατά του ΟΑΧΟ και των κυβερνοεπιθέσεων που έγιναν ευρέως γνωστές με τα ονόματα «WannaCry» και «NotPetya», καθώς και «Operation Cloud Horrege», ή παρείχαν υποστήριξη ή ενεπλάκησαν σε αυτές ή τις διευκόλυναν.
- (5) 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.

⁽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 1291 της 17.5.2019, σ. 13).

Άρθρο 2

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

Βρυξέλλες, 30 Ιουλίου 2020.

Για το Συμβούλιο
Ο Πρόεδρος
M. ROTH

ΠΑΡΑΡΤΗΜΑ

Τα ακόλουθα πρόσωπα και οντότητες ή φορείς προστίθενται στον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων και φορέων που παρατίθεται στο παράρτημα της απόφασης (ΚΕΠΠΑ) 2019/797:

«Α. Φυσικά πρόσωπα

	Όνομα	Στοιχεία ταυτότητας	Λόγοι	Ημερομηνία καταχώρισης
1.	GAO Qiang	<p>Τόπος γέννησης: Επαρχία Shandong, Κίνα</p> <p>Διεύθυνση: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China</p> <p>Ίθαγένεια: Κινεζική</p> <p>Φύλο: άρρεν</p>	<p>Ο Gao Qiang εμπλέκεται 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.</p> <p>Η “Operation Cloud Hopper” είχε ως στόχο συστήματα πληροφοριών πολυεθνικών εταιρειών σε έξι ηπείρους, συμπεριλαμβανομένων εταιρειών που βρίσκονται στην Ένωση, και απέκτησε πρόσβαση άνευ αδειας σε εμπορικά ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία.</p> <p>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”.</p> <p>Ο Gao Qiang μπορεί να συνδεθεί με τον APT10, μεταξύ άλλων μέσω της σχέσης του με την υποδομή διοίκησης και ελέγχου του APT10. Επιπλέον, η Huaying Haitai, οντότητα που καταχωρίστηκε εξαιτίας της παροχής υποστήριξης και της διευκόλυνσης της “Operation Cloud Hopper”, απασχολούσε τον Gao Qiang. Ο Gao Qiang συνδέεται με τον Zhang Shilong, ο οποίος έχει επίσης καταχωριστεί σε σχέση με την “Operation Cloud Hopper”. Ως εκ τούτου, ο Gao Qiang συνδέεται και με την Huaying Haitai και με τον Zhang Shilong.</p>	30.7.2020
2.	ZHANG Shilong	<p>Διεύθυνση: Hedong, Yuyang Road No 121, Tianjin, China</p> <p>Ίθαγένεια: Κινεζική</p> <p>Φύλο: άρρεν</p>	<p>Ο Zhang Shilong εμπλέκεται 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.</p> <p>Η “Operation Cloud Hopper” είχε ως στόχο συστήματα πληροφοριών πολυεθνικών εταιρειών σε έξι ηπείρους, συμπεριλαμβανομένων εταιρειών που βρίσκονται στην Ένωση, και απέκτησε πρόσβαση άνευ αδειας σε εμπορικά ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία.</p> <p>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”.</p>	30.7.2020

			<p>Ο Zhang Shilong μπορεί να συνδεθεί 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, οντότητα που καταχωρίστηκε εξαιτίας της παροχής υποστήριξης και της διευκόλυνσης της “Operation Cloud Hopper”, απασχολούσε τον Zhang Shilong. Συνδέεται με τον Gao Qiang, ο οποίος έχει επίσης καταχωριστεί σε σχέση με την “Operation Cloud Hopper”. Ως εκ τούτου, ο Zhang Shilong συνδέεται και με την Huaying Haitai και με τον Gao Qiang.</p>	
3.	Alexey Valeryevich MININ	<p>Алексей Валерьевич МИНИН</p> <p>Ημερομηνία γέννησης: 27 Μαΐου 1972</p> <p>Τόπος γέννησης: Περιφέρεια Perm, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία)</p> <p>Αριθ. διαβατηρίου: 120017582</p> <p>Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας</p> <p>Ισχύς: από 17 Απριλίου 2017 έως 17 Απριλίου 2022</p> <p>Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία</p> <p>Ίθαγένεια: Ρωσική</p> <p>Φύλο: άρρεν</p>	<p>Ο Alexey Minin συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες.</p> <p>Ως υπεύθυνος υποστήριξης για πληροφορίες από ανθρώπινο υλικό της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Alexey Minin ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδειας στο δίκτυο WiFi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσει την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020
4.	Aleksei Sergeyvich MORENETS	<p>Алексей Валерьевич МИНИН</p> <p>Ημερομηνία γέννησης: 31 Ιουλίου 1977</p> <p>Τόπος γέννησης: Περιφέρεια Murmanskaya, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία)</p> <p>Αριθ. διαβατηρίου: 100135556</p> <p>Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας</p> <p>Ισχύς από: 17 Απριλίου 2017 έως 17 Απριλίου 2022</p> <p>Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία</p> <p>Ίθαγένεια: Ρωσική</p> <p>Φύλο: άρρεν</p>	<p>Ο Aleksei Morenets συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες.</p> <p>Ως χειριστής κυβερνοχώρου της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Aleksei Morenets ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδειας στο δίκτυο WiFi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσει την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	<p>Евгений Михайлович СЕРЕБРЯКОВ</p> <p>Ημερομηνία γέννησης: 26 Ιουλίου 1981</p> <p>Τόπος γέννησης: Kursk, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία)</p> <p>Αριθ. διαβατηρίου: 100135555</p> <p>Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας</p> <p>Ισχύς: από 17 Απριλίου 2017 έως 17 Απριλίου 2022</p> <p>Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία</p> <p>Ίθαγένεια: Ρωσική</p> <p>Φύλο: άρρεν</p>	<p>Ο Evgenii Serebriakov συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες.</p> <p>Ως χειριστής κυβερνοχώρου της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Evgenii Serebriakov ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδειας στο δίκτυο Wi-Fi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	<p>Олег Михайлович СОТНИКОВ</p> <p>Ημερομηνία γέννησης: 24 Αυγούστου 1972</p> <p>Τόπος γέννησης: Ульяновск, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία)</p> <p>Αριθ. διαβατηρίου: 120018866</p> <p>Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας</p> <p>Ισχύς από: 17 Απριλίου 2017 έως 17 Απριλίου 2022</p> <p>Τόπος εργασίας: Μόσχα, Ρωσική Ομοσπονδία</p> <p>Ίθαγένεια: Ρωσική</p> <p>Φύλο: άρρεν</p>	<p>Ο Oleg Sotnikov συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικές σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες.</p> <p>Ως υπεύθυνος υποστήριξης για πληροφορίες από ανθρώπινο υλικό της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Oleg Sotnikov ανήκε σε ομάδα τεσσάρων μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχειρήσαν να αποκτήσουν πρόσβαση άνευ αδειας στο δίκτυο WiFi του ΟΑΧΟ στη Χάγη, στις Κάτω Χώρες, τον Απρίλιο του 2018. Η απόπειρα κυβερνοεπίθεσης είχε ως στόχο την πειρατεία στο δίκτυο WiFi του ΟΑΧΟ και, σε περίπτωση επιτυχίας, θα έθετε σε κίνδυνο την ασφάλεια του δικτύου και τις διεξαγόμενες έρευνες του ΟΑΧΟ. Η Υπηρεσία Αμυντικών Πληροφοριών και Ασφάλειας των Κάτω Χωρών (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) αναχαιτίσε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.</p>	30.7.2020

B. Νομικά πρόσωπα, οντότητες και φορείς

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	<p>Άλλως: Haitai Technology Development Co. Ltd</p> <p>Τόπος εγκατάστασης: Tianjin, Κίνα</p>	<p>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.</p>	30.7.2020

			<p>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 εμπορικά ευαίσθητα δεδομένα, με αποτέλεσμα σημαντική οικονομική ζημία.</p> <p>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”.</p> <p>Η Huaying Haitai μπορεί να συνδεθεί με τον APT10. Επίσης, η Huaying Haitai απασχολούσε τον Gao Qiang και τον Zhang Shilong· αμφότεροι έχουν καταχωριστεί σε σχέση με την “Operation Cloud Hopper”. Ως εκ τούτου, η Huaying Haitai συνδέεται με τον Gao Qiang και τον Zhang Shilong.</p>	
2.	Chosun Expo	<p>Άλλως: Chosen Expo, Korea Export Joint Venture</p> <p>Τόπος εγκατάστασης: ΛΔΚ</p>	<p>Η Chosun Expo παρείχε οικονομική, τεχνική ή υλική υποστήριξη και διευκόλυνε 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, συμπεριλαμβανομένων των κυβερνοεπιθέσεων που έγιναν ευρέως γνωστές ως “WannaCry” και των κυβερνοεπιθέσεων κατά της Πολωνικής Αρχής Χρηματοπιστωτικής Εποπτείας και της Sony Pictures Entertainment, καθώς και κυβερνοκλοπής από την Bangladesh Bank και απόπειρας κυβερνοκλοπής από τη Vietnam Tien Phong Bank.</p> <p>Η “WannaCry” διατάραξε τη λειτουργία των συστημάτων πληροφοριών σε παγκόσμιο επίπεδο, στοχεύοντας σε συστήματα πληροφοριών με λυτριστικό και εμποδίζοντας την πρόσβαση σε δεδομένα. Επηρέασε τα συστήματα πληροφοριών εταιρειών στην Ένωση, συμπεριλαμβανομένων των συστημάτων πληροφοριών που σχετίζονται με υπηρεσίες αναγκαίες για τη διατήρηση βασικών υπηρεσιών και οικονομικών δραστηριοτήτων στο εσωτερικό κρατών μελών.</p> <p>Ο παράγων που είναι ευρέως γνωστός ως “APT38” (“Advanced persistent Threat 38”) ή η “Lazarus Group” διεξήγαγε την “WannaCry”.</p> <p>Η Chosun Expo μπορεί να συνδεθεί με τον APT38/τη Lazarus Group, μεταξύ άλλων μέσω των λογαριασμών που χρησιμοποιούνται για τις κυβερνοεπιθέσεις.</p>	30.7.2020
3.	Κύριο Κέντρο Ειδικών Τεχνολογιών (GTsST) της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU)	Διεύθυνση: 22 Kirova Street, Moscow, Russian Federation	<p>Το Κύριο Κέντρο Ειδικών Τεχνολογιών (GTsST) της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), γνωστό και με τον αριθμό αναφοράς 74455, είναι υπεύθυνο για κυβερνοεπιθέσεις με σημαντικές επιπτώσεις που προήλθαν από χώρες εκτός της Ένωσης και αποτέλεσαν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της, καθώς και για κυβερνοεπιθέσεις με σημαντικές επιπτώσεις εις βάρος τρίτων κρατών, συμπεριλαμβανομένων των κυβερνοεπιθέσεων που έγιναν ευρέως γνωστές ως “NotPetya” ή “EternalPetya” του Ιουνίου του 2017 και των κυβερνοεπιθέσεων με στόχο ουκρανικό δίκτυο ηλεκτρικής ενέργειας τον χειμώνα του 2015 και του 2016.</p>	30.7.2020»

		<p>Η “NotPetya” ή “EternalPetya” στέρησε από διάφορες εταιρείες στην Ένωση, στην ευρύτερη Ευρώπη και παγκοσμίως την πρόσβαση σε δεδομένα, στοχεύοντας υπολογιστές με λυτρισμικό και εμποδίζοντας την πρόσβαση σε δεδομένα, με αποτέλεσμα, μεταξύ άλλων, σημαντική οικονομική ζημία. Η κυβερνοεπίθεση σε ουκρανικό δίκτυο ηλεκτρικής ενέργειας είχε ως αποτέλεσμα τη διακοπή της λειτουργίας ορισμένων τμημάτων του κατά τη διάρκεια του χειμώνα.</p> <p>Ο παράγων που είναι ευρέως γνωστός ως “Sandworm” (άλλως “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” και “Telebots”), ο οποίος είναι επίσης υπεύθυνος για την επίθεση στο ουκρανικό δίκτυο ηλεκτρικής ενέργειας, διεξήγαγε τη “NotPetya” ή “EternalPetya”.</p> <p>Το Κύριο Κέντρο Ειδικών Τεχνολογιών της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας διαδραματίζει ενεργό ρόλο στις δραστηριότητες στον κυβερνοχώρο που αναλαμβάνει ο Sandworm και μπορεί να συνδεθεί με τον Sandworm.</p>	
--	--	---	--

ISSN 1977-0669 (ηλεκτρονική έκδοση)
ISSN 1725-2547 (έντυπη έκδοση)



Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης
2985 Λουξεμβούργο
ΛΟΥΞΕΜΒΟΥΡΓΟ

EL