2024/1391

17.5.2024

ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2024/1391 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 17ης Μαΐου 2024

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) Η απόφαση (ΚΕΠΠΑ) 2019/797 ισχύει έως τις 18 Μαΐου 2025. Βάσει επανεξέτασης της εν λόγω απόφασης, η ισχύς των περιοριστικών μέτρων που ορίζονται σε αυτή θα πρέπει να παραταθεί έως την εν λόγω ημερομηνία.

(3) Δεδομένου ότι η κακόβουλη συμπεριφορά στον κυβερνοχώρο συνεχίζεται και επιτείνεται, μεταξύ άλλων με συμπεριφορές που στρέφονται κατά τρίτων κρατών, οι λόγοι για τη συμπερίληψη έξι προσώπων και δύο οντοτήτων στον κατάλογο των φυσικών και νομικών προσώπων, οντοτήτων και φορέων που υπόκεινται σε περιοριστικά μέτρα του παραρτήματος του κανονισμού (ΕΕ) 2019/797 θα πρέπει να επικαιροποιηθούν.

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

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Η απόφαση (ΚΕΠΠΑ) 2019/797 τροποποιείται ως εξής:

1) Το άρθρο 10 αντικαθίσταται από το ακόλουθο κείμενο:

«Άρθρο 10

Η παρούσα απόφαση ισχύει έως τις 18 Μαΐου 2025 και τελεί υπό διαρκή επανεξέταση.»·

2) Το παράρτημα τροποποιείται σύμφωνα με το παράρτημα της παρούσας απόφασης.

Άρθρο 2

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

Βρυξέλλες, 17 Μαΐου 2024.

Για το Συμβούλιο

Η Πρόεδρος

H. LAHBIB

([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).

ΠΑΡΑΡΤΗΜΑ

Το παράρτημα της απόφασης (ΚΕΠΠΑ) 2019/797 («Κατάλογος των φυσικών και νομικών προσώπων, οντοτήτων και φορέων που αναφέρονται στα άρθρα 4 και 5») τροποποιείται ως εξής:

1. Στον κατάλογο με τίτλο «Α. Φυσικά πρόσωπα», οι καταχωρίσεις 3 έως 8 αντικαθίστανται από το ακόλουθο κείμενο:

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
«3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Ημερομηνία γέννησης: 27.5.1972 Τόπος γέννησης: Περιφέρεια Perm, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 120017582 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς: από 17.4.2017 έως 17.4.2022 Τόπος εγκατάστασης: Μόσχα, Ρωσική Ομοσπονδία Ιθαγένεια: Ρωσική Φύλο: άρρεν	Ο Alexey Minin συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικά σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες και σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτων χωρών. 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 τετραμελή ομάδα της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών που επιχείρησαν 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 Wi-Fi 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ. Σώμα ενόρκων της Δυτικής Περιφέρειας της Πενσυλβανίας (Ηνωμένες Πολιτείες της Αμερικής) απήγγειλε κατηγορίες κατά του Alexey Minin ως αξιωματικού της Ρωσικής Κεντρικής Διεύθυνσης Πληροφοριών (GRU), για αθέμιτη χρησιμοποίηση δεδομένων καταχωρημένων σε ηλεκτρονικούς υπολογιστές, ηλεκτρονική απάτη, διακεκριμένη κλοπή ταυτότητας και νομιμοποίηση εσόδων από παράνομες δραστηριότητες.	30.7.2020

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Ημερομηνία γέννησης: 31.7.1977 Τόπος γέννησης: Περιφέρεια (όμπλαστ) Murmanskaya, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 100135556 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς: από 17.4.2017 έως 17.4.2022 Τόπος εγκατάστασης: Μόσχα, Ρωσική Ομοσπονδία Ιθαγένεια: Ρωσική Φύλο: άρρεν	Ο Aleksei Morenets συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικά σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες και σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτων χωρών. 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 επιχείρησαν 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 Wi-Fi 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ. Σώμα ενόρκων της Δυτικής Περιφέρειας της Πενσυλβανίας (Ηνωμένες Πολιτείες της Αμερικής) απήγγειλε κατηγορίες κατά του Aleksei Morenets ως διορισμένου στη Στρατιωτική Μονάδα 26165, για αθέμιτη χρησιμοποίηση δεδομένων καταχωρημένων σε ηλεκτρονικούς υπολογιστές, ηλεκτρονική απάτη, διακεκριμένη κλοπή ταυτότητας και νομιμοποίηση εσόδων από παράνομες δραστηριότητες.	30.7.2020

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Ημερομηνία γέννησης: 26.7.1981 Τόπος γέννησης: Kursk, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 100135555 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς: από 17.4.2017 έως 17.4.2022 Τόπος εγκατάστασης: Μόσχα, Ρωσική Ομοσπονδία Ιθαγένεια: Ρωσική Φύλο: άρρεν	Ο Evgenii Serebriakov συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικά σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες και σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτων χωρών. 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 επιχείρησαν 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 Wi-Fi 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ. Από την άνοιξη του 2022 ο Evgenii Serebriakov ηγείται της “Sandworm” (άλλως “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” και “Telebots”), μιας ομάδας πρακτόρων και χάκερ που συνδέεται με τη Μονάδα 74455 της Κεντρικής Διεύθυνσης Πληροφοριών της Ρωσίας. Μετά την έναρξη του επιθετικού πολέμου της Ρωσίας κατά της Ουκρανίας η Sandworm πραγματοποίησε κυβερνοεπιθέσεις κατά της Ουκρανίας, μεταξύ άλλων κατά ουκρανικών κυβερνητικών υπηρεσιών.	30.7.2020

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Ημερομηνία γέννησης: 24.8.1972 Τόπος γέννησης: Ulyanovsk, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Αριθ. διαβατηρίου: 120018866 Εκδοθέν από: Υπουργείο Εξωτερικών της Ρωσικής Ομοσπονδίας Ισχύς: από 17.4.2017 έως 17.4.2022 Τόπος εγκατάστασης: Μόσχα, Ρωσική Ομοσπονδία Ιθαγένεια: Ρωσική Φύλο: άρρεν	Ο Oleg Sotnikov συμμετείχε σε απόπειρα κυβερνοεπίθεσης με δυνητικά σημαντικές επιπτώσεις κατά του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες και σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτων χωρών. 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 επιχείρησαν 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 Wi-Fi 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ. Σώμα ενόρκων της Δυτικής Περιφέρειας της Πενσυλβανίας (Ηνωμένες Πολιτείες της Αμερικής) απήγγειλε κατηγορίες κατά του Oleg Sotnikov ως αξιωματικού της Ρωσικής Κεντρικής Διεύθυνσης Πληροφοριών (GRU), για αθέμιτη χρησιμοποίηση δεδομένων καταχωρημένων σε ηλεκτρονικούς υπολογιστές, ηλεκτρονική απάτη, διακεκριμένη κλοπή ταυτότητας και νομιμοποίηση εσόδων από παράνομες δραστηριότητες.	30.7.2020

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Ημερομηνία γέννησης: 15.11.1990 Τόπος γέννησης: Kursk, Ρωσική Σοβιετική Ομοσπονδιακή Δημοκρατία (νυν Ρωσική Ομοσπονδία) Ιθαγένεια: Ρωσική Φύλο: άρρεν	Ο Dmitry Badin συμμετείχε σε κυβερνοεπίθεση με σημαντικές επιπτώσεις κατά του Ομοσπονδιακού Κοινοβουλίου της Γερμανίας (Deutscher Bundestag) και σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτων χωρών. Ως αξιωματικός στρατιωτικών πληροφοριών του 85ου Κυρίου Κέντρου για Ειδικές Υπηρεσίες (GTsSS) της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), ο Dmitry Badin συμμετείχε σε ομάδα μελών της ρωσικής υπηρεσίας στρατιωτικών πληροφοριών, η οποία πραγματοποίησε κυβερνοεπίθεση κατά του Ομοσπονδιακού Κοινοβουλίου της Γερμανίας (Deutscher Bundestag) τον Απρίλιο και τον Μάιο του 2015. Η εν λόγω κυβερνοεπίθεση στόχευε το πληροφορικό σύστημα του κοινοβουλίου και επηρέασε τη λειτουργία του για αρκετές ημέρες. Εκλάπη σημαντικός όγκος δεδομένων ενώ επλήγησαν οι λογαριασμοί ηλεκτρονικού ταχυδρομείου μεγάλου αριθμού βουλευτών καθώς και της πρώην καγκελαρίου Άνγκελα Μέρκελ. Σώμα ενόρκων της Δυτικής Περιφέρειας της Πενσυλβανίας (Ηνωμένες Πολιτείες της Αμερικής) απήγγειλε κατηγορίες κατά του Dmitry Badin ως διορισμένου στη Στρατιωτική Μονάδα 26165, για αθέμιτη χρησιμοποίηση δεδομένων καταχωρημένων σε ηλεκτρονικούς υπολογιστές, ηλεκτρονική απάτη, διακεκριμένη κλοπή ταυτότητας και νομιμοποίηση εσόδων από παράνομες δραστηριότητες.	22.10.2020

ELI: http://data.europa.eu/eli/dec/2024/1391/oj

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Ημερομηνία γέννησης: 21.2.1961 Ιθαγένεια: Ρωσική Φύλο: άρρεν	Ο Igor Kostyukov είναι ο εν ενεργεία διοικητής της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), όπου προηγουμένως υπηρετούσε ως πρώτος αναπληρωτής διοικητής. Στη διοίκησή του υπάγεται και το 85ο κύριο κέντρο για Ειδικές Υπηρεσίες (GTsSS), (άλλως: “στρατιωτική μονάδα 26165” “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm”, και “Strontium”). Με την ιδιότητα αυτή, ο Igor Kostyukov είναι υπεύθυνος για τις κυβερνοεπιθέσεις που εξαπέλυσε το GTsSS, συμπεριλαμβανομένων εκείνων με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της. Ειδικότερα, αξιωματικοί στρατιωτικών πληροφοριών του GTsSS συμμετείχαν σε κυβερνοεπίθεση με στόχο το Ομοσπονδιακό Κοινοβούλιο της Γερμανίας (Deutscher Bundestag) τον Απρίλιο και τον Μάιο του 2015 και στην απόπειρα κυβερνοεπίθεσης που είχε ως στόχο την πειρατεία στο δίκτυο Wi-Fi του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες τον Απρίλιο του 2018. Η κυβερνοεπίθεση με στόχο το Ομοσπονδιακό Κοινοβούλιο της Γερμανίας στόχευε το πληροφορικό σύστημα του κοινοβουλίου και επηρέασε τη λειτουργία του για αρκετές ημέρες. Εκλάπη ένας σημαντικός όγκος δεδομένων ενώ επλήγησαν λογαριασμοί ηλεκτρονικού ταχυδρομείου μεγάλου αριθμού βουλευτών καθώς και της πρώην καγκελαρίου Άνγκελα Μέρκελ.	22.10.2020»

2. στον κατάλογο με τίτλο «Β. Νομικά πρόσωπα, οντότητες και φορείς», οι καταχωρίσεις 3 και 4 αντικαθίστανται από τις ακόλουθες:

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
«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	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, εμπλέκεται σε 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 που στόχο είχαν τρίτα κράτη, συμπεριλαμβανομένων των κυβερνοεπιθέσεων που έγιναν ευρέως γνωστές ως “NotPetya” ή “EternalPetya” τον Ιούνιο του 2017 και των κυβερνοεπιθέσεων με στόχο ουκρανικό δίκτυο ηλεκτρικής ενέργειας τον χειμώνα του 2015 και του 2016. 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.. Η ομάδα που είναι ευρέως γνωστή ως “Sandworm” (άλλως “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” και “Telebots”), η οποία είναι επίσης υπεύθυνη για την επίθεση στο ουκρανικό δίκτυο ηλεκτρικής ενέργειας, διεξήγαγε τη “NotPetya” ή “EternalPetya”. Μετά την έναρξη του επιθετικού πολέμου της Ρωσίας κατά της Ουκρανίας η Sandworm πραγματοποίησε κυβερνοεπιθέσεις κατά της Ουκρανίας, μεταξύ άλλων κατά ουκρανικών κυβερνητικών υπηρεσιών και ουκρανικών κρίσιμων υποδομών. Στις εν λόγω κυβερνοεπιθέσεις περιλαμβάνονται επιχειρήσεις στοχευμένου ηλεκτρονικού ψαρέματος και επιθέσεις με κακόβουλο λογισμικό και λυτρισμικό. 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 η Sandworm και μπορεί να συνδεθεί με την Sandworm	30.7.2020

	Όνομα	Πληροφορίες ταυτοποίησης	Λόγοι	Ημερομηνία καταχώρισης
4.	Κύριο Κέντρο για Ειδικές Υπηρεσίες (GTsSS) της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU)	Διεύθυνση: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	Το 85ο Κύριο Κέντρο για Ειδικές Υπηρεσίες (GTsSS) της Κεντρικής Διεύθυνσης του Γενικού Επιτελείου των Ενόπλων Δυνάμεων της Ρωσικής Ομοσπονδίας (GU/GRU), (άλλως "στρατιωτική μονάδα 26165" "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm", και "Strontium"), εμπλέκεται σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις οι οποίες συνιστούν εξωτερική απειλή για την Ένωση ή τα κράτη μέλη της και σε κυβερνοεπιθέσεις με σημαντικές επιπτώσεις κατά τρίτων κρατών. Ειδικότερα, αξιωματικοί στρατιωτικών πληροφοριών του GTsSS συμμετείχαν σε κυβερνοεπίθεση με στόχο το Ομοσπονδιακό Κοινοβούλιο της Γερμανίας (Deutscher Bundestag) τον Απρίλιο και τον Μάιο του 2015 και στην απόπειρα κυβερνοεπίθεσης που είχε ως στόχο την πειρατεία στο δίκτυο Wi-Fi του Οργανισμού για την Απαγόρευση των Χημικών Όπλων (ΟΑΧΟ) στις Κάτω Χώρες τον Απρίλιο του 2018. Η κυβερνοεπίθεση με στόχο το Ομοσπονδιακό Κοινοβούλιο της Γερμανίας στόχευε το πληροφορικό σύστημα του κοινοβουλίου και επηρέασε τη λειτουργία του για αρκετές ημέρες. Εκλάπη ένας σημαντικός όγκος δεδομένων ενώ επλήγησαν λογαριασμοί ηλεκτρονικού ταχυδρομείου μεγάλου αριθμού βουλευτών καθώς και της τότε καγκελαρίου Άνγκελα Μέρκελ. Μετά την έναρξη του επιθετικού πολέμου της Ρωσίας κατά της Ουκρανίας, η APT28 πραγματοποίησε κυβερνοεπιθέσεις κατά της Ουκρανίας (επιθέσεις στοχευμένου ηλεκτρονικού ψαρέματος και κακόβουλου λογισμικού).	22.10.2020»