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 ασφάλειας 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 εμπλεκομένους να σταματήσουν να προβαίνουν σε κακόβουλες κυβερνοδραστηριότητες που αποσκοπούν στην υπονόμευση της ακεραιότητας, της ασφάλειας 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 Hopper», 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 129Ι 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	Τόπος γέννησης: Επαρχία Shandong, Κίνα Διεύθυνση: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Ιθαγένεια: Κινεζική Φύλο: άρρεν	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 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". 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.	30.7.2020
2.	ZHANG Shilong	Διεύθυνση: Hedong, Yuyang Road No 121, Tianjin, China Ιθαγένεια: Κινεζική Φύλο: άρρεν	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 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".	30.7.2020

			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.	
3.	Alexey Valeryevich MININ	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	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 επιχείρησαν 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	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	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 επιχείρησαν 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	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	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 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 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	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 Ιθαγένεια: Ρωσική Φύλο: άρρεν	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 επιχείρησαν 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) αναχαίτισε την απόπειρα κυβερνοεπίθεσης, αποτρέποντας έτσι την πρόκληση σοβαρής βλάβης στον ΟΑΧΟ.	30.7.2020

Β. Νομικά πρόσωπα, οντότητες και φορείς

	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.	30.7.2020

			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 με τον Gao Qiang και τον Zhang Shilong.	
2.	Chosun Expo	Άλλως: Chosen Expo, Korea Export Joint Venture Τόπος εγκατάστασης: ΛΔΚ	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. 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. Ο παράγων που είναι ευρέως γνωστός ως “APT38” (“Advanced persistent Threat 38”) ή η “Lazarus Group” διεξήγαγαν την “WannaCry”. Η Chosun Expo μπορεί να συνδεθεί με τον APT38/τη Lazarus Group, μεταξύ άλλων μέσω των λογαριασμών που χρησιμοποιούνται για τις κυβερνοεπιθέσεις.	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	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.	30.7.2020»

			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. 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”. 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.	