EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ΤΟΠΙΟ ΑΠΕΙΛΩΝ ΤΟΥ ENISA ΓΙΑ ΤΟ 2021

Απρίλιος 2020 έως μέσα Ιουλίου 2021

ΟΚΤΩΒΡΙΟΣ 2021

ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟΝ ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, είναι ο οργανισμός της Ένωσης που αποσκοπεί να διασφαλίσει υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια, που ιδρύθηκε το 2004 και ενισχύθηκε από την Πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στη χάραξη της πολιτικής της ΕΕ στον τομέα του κυβερνοχώρου, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της ανάπτυξης ικανοτήτων και της αύξησης της εγρήγορσης, ο Οργανισμός συνεργάζεται με τους βασικούς ενδιαφερόμενους φορείς για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την υποστήριξη της ανθεκτικότητας των υποδομών της Ένωσης και, τελικά, τη διατήρηση της ψηφιακής ασφάλειας για την κοινωνία και τους πολίτες της Ευρώπης. Περισσότερες πληροφορίες για τον ENISA και το έργο του διατίθενται εδώ: www.enisa.europa.eu.

ΕΠΙΚΟΙΝΩΝΙΑ

Για να επικοινωνήσετε με τους συντάκτες, χρησιμοποιήστε τη διεύθυνση etl@enisa.europa.eu.
Για πληροφορίες σχετικά με το παρόν έγγραφο, χρησιμοποιήστε τη διεύθυνση press@enisa.europa.eu.

ΣΥΝΤΑΚΤΕΣ

Ιφιγένεια Λέλλα, Μαριάνθη Θεοχαρίδου, Ελένη Τσεκμεζόγλου, Απόστολος Μαλάτρας – Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

ΣΥΝΤΕΛΕΣΤΕΣ

Claudio Ardagna, Stephen Corbiaux, Ανδρέας Σφακιανάκης, Χρήστος Δουλγέρης

ΕΥΧΑΡΙΣΤΙΕΣ

Θα θέλαμε να ευχαριστήσουμε τα μέλη και τους παρατηρητές της ad hoc ομάδας εργασίας του ENISA για τα τοπία των κυβερνοαπειλών για τις πολύτιμες παρατηρήσεις και τα σχόλιά τους κατά την επικύρωση της παρούσας έκθεσης. Ευχαριστούμε τη συμβουλευτική ομάδα του ENISA και το δίκτυο των εθνικών υπαλλήλων-συνδέσμων για την πολύτιμη ανατροφοδότησή τους.
Θα θέλαμε επίσης να ευχαριστήσουμε τις ομάδες επίγνωσης της κατάστασης και κοινοποίησης συμβάντων του ENISA για την ενεργό συμβολή και υποστήριξή τους στην ενοποίηση διαφόρων πληροφοριών στο τοπίο των απειλών.

ΝΟΜΙΚΗ ΓΝΩΣΤΟΠΟΙΗΣΗ

Πρέπει να ληφθεί υπόψη ότι η παρούσα δημοσίευση εκφράζει τις απόψεις και τις ερμηνείες του ENISA, εκτός εάν αναφέρεται διαφορετικά. Η παρούσα δημοσίευση δεν πρέπει να εκληφθεί ως νομική πράξη του ENISA ή των οργάνων του ENISA, εκτός εάν εγκριθεί σύμφωνα με τον κανονισμό (ΕΕ) 2019/881. Ο ENISA μπορεί να επικαιροποιεί την παρούσα δημοσίευση κατά καιρούς.

Πηγές τρίτων αναφέρονται κατά περίπτωση. Ο ENISA δεν φέρει ευθύνη για το περιεχόμενων των εξωτερικών πηγών, συμπεριλαμβανομένων των εξωτερικών ιστότοπων που αναφέρονται στην παρούσα έκδοση.

Η παρούσα έκδοση προορίζεται αποκλειστικά για ενημερωτικούς σκοπούς. Η πρόσβαση σε αυτήν πρέπει να είναι δωρεάν. Ο ENISA και τα πρόσωπα που ενεργούν για λογαριασμό του δεν φέρουν ευθύνη για τη χρήση των πληροφοριών που περιέχονται στην παρούσα έκδοση.

ΔΗΛΩΣΗ ΠΕΡΙ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

© Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), 2021
Επιτρέπεται η αναπαραγωγή με αναφορά της πηγής. Για κάθε χρήση ή αναπαραγωγή φωτογραφιών ή άλλου υλικού που δεν υπόκειται στους κανόνες του ENISA για τα δικαιώματα πνευματικής ιδιοκτησίας, πρέπει να ζητείται απευθείας η άδεια των κατόχων των δικαιωμάτων πνευματικής ιδιοκτησίας.

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΟΨΗ

Πρόκειται για την ένατη έκδοση της έκθεσης του ENISA σχετικά με το τοπίο των απειλών (ETL), μια ετήσια έκθεση σχετικά με την κατάσταση του τοπίου των κυβερνοαπειλών, η οποία εντοπίζει τις βασικές απειλές, τις μείζονες τάσεις που παρατηρούνται όσον αφορά τις απειλές, τους παράγοντες απειλών και τις τεχνικές επιθέσεων, και η οποία περιγράφει επίσης τα σχετικά μέτρα μετριασμού. Στο πλαίσιο της διαδικασίας συνεχούς βελτίωσης της μεθοδολογίας μας για την ανάπτυξη του τοπίου των απειλών, οι φετινές εργασίες υποστηρίχθηκαν από μια νεοσυσταθείσα ad hoc ομάδα εργασίας του ENISA για τα τοπία των απειλών για την ασφάλεια στον κυβερνοχώρο (CTL).

Η έκθεση ETL 2021 καλύπτει το χρονικό διάστημα από τον Απρίλιο του 2020 έως τον Ιούλιο του 2021 το οποίο αναφέρεται σε όλη την έκθεση ως «περίοδος αναφοράς» . Κατά την περίοδο αναφοράς εντοπίστηκαν οι εξής βασικές απειλές :

- **Λυτρισμικό**
- **Κακόβουλο λογισμικό**
- **Cryptojacking (εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση)**
- **Απειλές που σχετίζονται με το ηλεκτρονικό ταχυδρομείο**
- **Απειλές κατά των δεδομένων**
- **Απειλές κατά της διαθεσιμότητας και της ακεραιότητας**
- **Παραπληροφόρηση – εσφαλμένη πληροφόρηση**
- **Μη κακόβουλες απειλές**
- **Επιθέσεις στην αλυσίδα εφοδιασμού**

Στην παρούσα έκθεση εξετάζουμε τις πρώτες 8 κατηγορίες απειλών για την κυβερνοασφάλεια. Οι απειλές στην αλυσίδα εφοδιασμού, η 9η κατηγορία, αναλύθηκαν λεπτομερώς, λόγω της ιδιαίτερης προβολής τους, σε ειδική έκθεση του ENISA με τίτλο «ENISA Threat landscape for Supply Chain Attacks» (Τοπίο των απειλών για τις επιθέσεις στην αλυσίδα εφοδιασμού του ENISA) [1].

Για καθεμία από τις απειλές που εντοπίστηκαν, αναλύονται οι τεχνικές επίθεσης, τα αξιοσημείωτα συμβάντα και οι τάσεις μαζί με τα προτεινόμενα μέτρα μετριασμού. Όσον αφορά τις τάσεις, κατά την περίοδο αναφοράς επισημαίνουμε τα ακόλουθα:

- Το **λυτρισμικό** έχει αξιολογηθεί ως η **βασική απειλή για την περίοδο 2020-2021**.
- **Οι κυβερνητικοί οργανισμοί έχουν εντείνει τις προσπάθειές τους** σε εθνικό και διεθνές επίπεδο.
- **Οι εγκληματίες του κυβερνοχώρου υποκινούνται όλο και περισσότερο από τη χρηματοποίηση** των δραστηριοτήτων τους, π.χ. λυτρισμικό. Το **κρυπτονόμισμα** παραμένει η συνηθέστερη μέθοδος πληρωμής για τους παράγοντες απειλής.
- Η **μείωση των επιθέσεων κακόβουλου λογισμικού** που παρατηρήθηκε το 2020 συνεχίζεται κατά τη διάρκεια του 2021. Το 2021 διαπιστώσαμε αύξηση των παραγόντων απειλής που καταφεύγουν σε σχετικά νέες ή ασυνήθιστες γλώσσες προγραμματισμού για τη μεταφορά του κώδικά τους.
- Σε σύγκριση με τα τελευταία έτη, το πρώτο τρίμηνο του 2021 ο αριθμός **μολύνσεων από λογισμικό cryptojacking** κατέγραψε **πρωτοφανές υψηλό επίπεδο**. Το **οικονομικό κέρδος** που συνδέεται με την εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση παρείχε κίνητρα στους παράγοντες απειλής να πραγματοποιήσουν τις εν λόγω επιθέσεις.
- **Η νόσος COVID-19 εξακολουθεί να αποτελεί το κυρίαρχο δόλωμα στις εκστρατείες** επιθέσεων ηλεκτρονικού ταχυδρομείου.
- Σημειώθηκε **απότομη αύξηση των παραβιάσεων δεδομένων που σχετίζονται με τον τομέα της υγειονομικής περίθαλψης**.

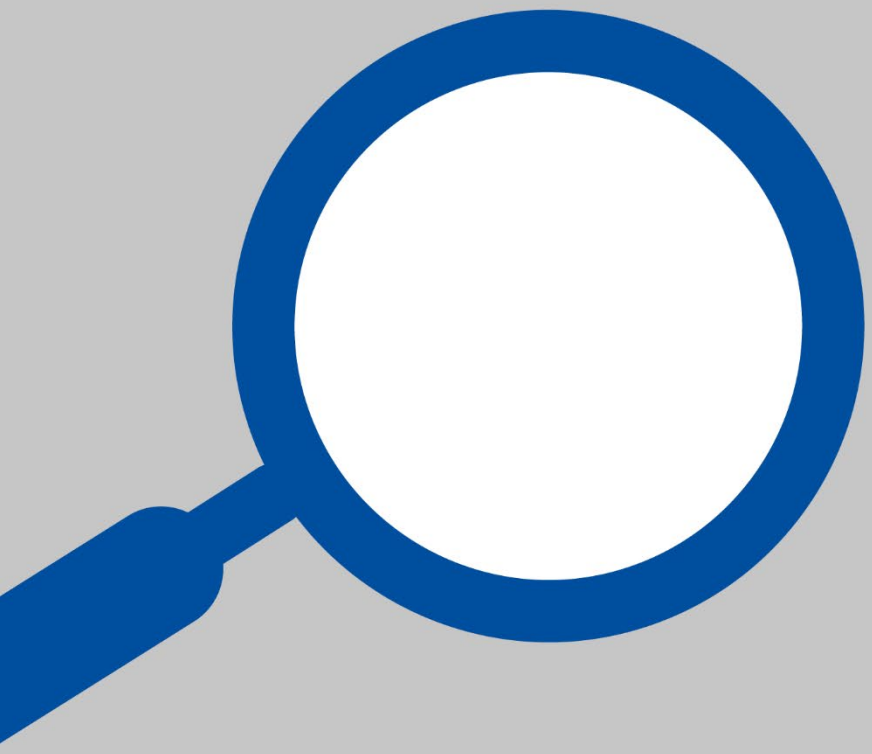
[1] ENISA Threat Landscape for Supply Chain Attacks, Ιούλιος 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- **Οι παραδοσιακές εκστρατείες DDoS (Distributed Denial of Service - κατανεμημένης επίθεσης άρνησης υπηρεσίας)** το 2021 είναι πιο στοχευμένες, πιο επίμονες και όλο και περισσότερο με πολλαπλούς φορείς επίθεσης. Το **ΔτΠ (διαδίκτυο των πραγμάτων)** σε συνδυασμό με τα **δίκτυα κινητής τηλεφωνίας** έχει ως αποτέλεσμα ένα νέο κύμα επιθέσεων DDoS.
- Το 2020 και το 2021 παρατηρούμε **απότομη αύξηση των μη κακόβουλων περιστατικών**, καθώς η πανδημία COVID-19 κατέστη πολλαπλασιαστής των **ανθρωπίνων σφαλμάτων** και των **εσφαλμένων ρυθμίσεων συστήματος**, σε σημείο που οι περισσότερες παραβάσεις το 2020 προκλήθηκαν από σφάλματα.

Η κατανόηση των τάσεων που σχετίζονται με τους παράγοντες απειλών, τα κίνητρά τους και τους στόχους τους συμβάλλει σημαντικά στον σχεδιασμό αμυντικών δράσεων κυβερνοασφάλειας και στρατηγικών μετριασμού. Αυτό αποτελεί αναπόσπαστο μέρος της συνολικής αξιολόγησης των απειλών, δεδομένου ότι επιτρέπει την ιεράρχηση των ελέγχων ασφαλείας και τη χάραξη ειδικής στρατηγικής με βάση τον δυνητικό αντίκτυπο και την πιθανότητα υλοποίησης της απειλής. Στο πλαίσιο αυτό, για τους σκοπούς της ETL 2021, λαμβάνονται υπόψη οι ακόλουθες τέσσερις κατηγορίες παραγόντων απειλών κατά της κυβερνοασφάλειας:

- **Φορείς που χρηματοδοτούνται από το κράτος**
- **Δράστες κυβερνοεγκλήματος**
- **Χάκερ που προσφέρουν τις υπηρεσίες τους επ' αμοιβή**
- **Χακτιβιστές**

Μέσω συνεχούς ανάλυσης, ο ENISA προέβη στην εξαγωγή τάσεων και σημείων ενδιαφέροντος για καθεμία από τις μείζονες απειλές που παρουσιάζονται στην έκθεση ETL 2021. Τα βασικά πορίσματα και οι διαπιστώσεις της παρούσας αξιολόγησης βασίζονται σε πολλαπλούς και δημόσια διαθέσιμους πόρους, οι οποίοι παρέχονται στις βιβλιογραφικές πηγές που χρησιμοποιήθηκαν για την κατάρτιση του παρόντος εγγράφου. Η έκθεση απευθύνεται κυρίως σε στρατηγικούς φορείς λήψης αποφάσεων και φορείς χάραξης πολιτικής, ωστόσο πρόκειται να αποτελέσει αντικείμενο ενδιαφέροντος και για την τεχνική κοινότητα στον τομέα της κυβερνοασφάλειας.



ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ ΤΟΠΙΟΥ ΤΩΝ ΑΠΕΙΛΩΝ

Στην ένατη έκδοσή της, η έκθεση του ENISA για το τοπίο των απειλών (ETL) παρέχει μια γενική επισκόπηση του τοπίου απειλών στον κυβερνοχώρο. Η έκθεση ETL είναι εν μέρει στρατηγικής και εν μέρει τεχνικής φύσεως, με πληροφορίες που αφορούν αναγνώστες τόσο εξοικειωμένους όσο και μη εξοικειωμένους με τεχνικά θέματα. Οι φετινές εργασίες υποστηρίχθηκαν από μια νεοσυσταθείσα ad hoc ομάδα εργασίας του ENISA για τα τοπία των απειλών στον κυβερνοχώρο (CTL)[2].

Οι επιθέσεις στον κυβερνοχώρο εξακολουθούν να αυξάνονται κατά τα έτη 2020 και 2021, όχι μόνο από πλευράς φορέων και αριθμών, αλλά και από την άποψη του αντικτύπου τους. Η πανδημία COVID-19 είχε επίσης – αναμενόμενα- αντίκτυπο στο τοπίο των απειλών στον κυβερνοχώρο. Μία από τις πλέον διαρκείς εξελίξεις που προέκυψαν από την πανδημία COVID-19 είναι μια διαρκής μετάβαση σε ένα υβριδικό μοντέλο εργασίας γραφείου. Ως εκ τούτου, οι απειλές στον κυβερνοχώρο που σχετίζονται με την πανδημία και εκμεταλλεύονται τη «νέα κανονικότητα» γίνονται πλέον κυρίαρχη τάση. Η τάση αυτή έχει αυξήσει την επιφάνεια έκθεσης σε πιθανές επιθέσεις και, ως εκ τούτου, παρατηρήθηκε αύξηση του αριθμού των κυβερνοεπιθέσεων που στρέφονται κατά οργανισμών και εταιρειών μέσω της εργασίας από το σπίτι[3].

Σε γενικές γραμμές, οι απειλές για την ασφάλεια στον κυβερνοχώρο βρίσκονται σε άνοδο. Υποκινούνται από τη διαρκώς αυξανόμενη διαδικτυακή παρουσία, τη μετάβαση των παραδοσιακών υποδομών σε επιγραμμικές λύσεις και λύσεις που βασίζονται στο υπολογιστικό νέφος, την προηγμένη διασυνδεσιμότητα και την εκμετάλλευση νέων χαρακτηριστικών αναδυόμενων τεχνολογιών, όπως η τεχνητή νοημοσύνη (TN)[4][5], ενώ το τοπίο των απειλών κυβερνοασφάλειας είναι διευρυμένο όσον αφορά τόσο την ποικιλομορφία των επιθέσεων, όσο και την πολυπλοκότητά τους και τον αντίκτυπό τους. Ειδικότερα, οι απειλές για τις αλυσίδες εφοδιασμού και η σημασία τους λόγω των δυνητικά καταστροφικών αλυσιδωτών επιπτώσεών τους έχουν καταλάβει την υψηλότερη θέση μεταξύ των μειζόνων απειλών, σε τόσο μεγάλο βαθμό ώστε ο ENISA δημιούργησε ειδικό τοπίο απειλών για την εν λόγω κατηγορία απειλών[6].

Αξίζει να σημειωθεί ότι, στην παρούσα έκδοση της έκθεσης ETL, δόθηκε ιδιαίτερη έμφαση στον αντίκτυπο των κυβερνοαπειλών σε διάφορους τομείς, συμπεριλαμβανομένων εκείνων που απαριθμούνται στην οδηγία για την ασφάλεια δικτύων και πληροφοριών (οδηγία NIS). Ενδιαφέρουσες γνώσεις μπορούν να αντληθούν από τις ιδιαιτερότητες κάθε τομέα όσον αφορά το τοπίο των απειλών, καθώς και από πιθανές αλληλεξαρτήσεις και σημαντικούς τομείς. Ως εκ τούτου, τα τοπία των τομεακών απειλών χρήζουν περαιτέρω προσοχής.

Φέτος πραγματοποιήθηκαν επίσης ορισμένα αξιοσημείωτα βήματα από την πλευρά των υπερασπιστών στην κοινότητα του κυβερνοχώρου, καθώς και από τους υπεύθυνους χάραξης πολιτικής. Η παγκόσμια κοινότητα έχει αρχίσει να συνειδητοποιεί τη σημασία της επικοινωνίας και της συνεργασίας για την εξέταση και την παρακολούθηση των εγκληματιών του κυβερνοχώρου, με το λυτρισμικό (η σημαντικότερη απειλή για την περίοδο αναφοράς της ETL 2021) ιδίως να αποτελεί πρωταρχικό θέμα στις ημερήσιες διατάξεις των συνεδριάσεων σχετικά με τη στρατηγική μεταξύ παγκόσμιων ηγετών.

Οι συστηματικοί αναγνώστες προηγούμενων εκδόσεων της ETL 2021 θα διαπιστώσουν διαφορά στη χαρτογράφηση των κύριων απειλών. Φέτος, ο ENISA έκανε ένα βήμα προς τα πίσω και προέβη στην ενοποίηση κατηγοριών απειλών με σκοπό την ενσωμάτωση και την καλύτερη εκπροσώπηση παρόμοιων απειλών. Η ενέργεια αυτή

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Cost of a Data Breach Report 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA AI Threat Landscape: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] ENISA Threat Landscape for Supply Chain Attacks, Ιούλιος 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

αποτελεί μέρος των συνεχιζόμενων προσπαθειών με σκοπό την επαναταξινόμηση των απειλών και πρόκειται να συμβάλει στον καθορισμό μεθοδολογικών τάσεων κατά τα προσεχή έτη.

Η έκθεση ETL 2021 βασίζεται σε διάφορες πηγές πληροφοριών ανοικτής πηγής και σε πηγές υπηρεσιών παροχής πληροφοριών σχετικά με απειλές στον κυβερνοχώρο. Εντοπίζει μείζονες απειλές, τάσεις και ευρήματα και παρέχει σχετικές στρατηγικές μετριασμού υψηλού επιπέδου. Στην παρούσα φάση ο ENISA πραγματοποιεί εργασίες για την εδραίωση της μεθοδολογίας για την υποβολή εκθέσεων σχετικά με το τοπίο των απειλών με σκοπό την προώθηση της διαφάνειας και της συνέπειας στις εργασίες.

1.1. ΒΑΣΙΚΕΣ ΑΠΕΙΛΕΣ

Κατά τη διάρκεια του 2020 και του 2021 εμφανίστηκαν και υλοποιήθηκαν διάφορες κυβερνοαπειλές. Με βάση την ανάλυση που παρουσιάζεται στην παρούσα έκθεση, το τοπίο απειλών του ENISA για το 2021 προσδιορίζει και επικεντρώνεται στις ακόλουθες 8 ομάδες βασικών απειλών (βλ. Διάγραμμα 1). Οι 8 αυτές ομάδες απειλών επισημαίνονται λόγω της δημόσιας προβολής τους κατά την περίοδο αναφοράς, της δημοτικότητας τους και του αντικτύπου που είχε η υλοποίηση των εν λόγω απειλών.

- **Λυτρισμικό**
  Το λυτρισμικό είναι ένα είδος κακόβουλων επιθέσεων κατά τις οποίες οι επιτιθέμενοι κρυπτογραφούν τα δεδομένα ενός οργανισμού και απαιτούν πληρωμή για την αποκατάσταση της πρόσβασης. Το λυτρισμικό υπήρξε η βασική απειλή κατά την περίοδο αναφοράς, με αρκετά περιστατικά υψηλής προβολής και δημοσιότητας. Η σημασία και ο αντίκτυπος της απειλής του λυτρισμικού αποδεικνύονται επίσης από μια σειρά σχετικών πρωτοβουλιών πολιτικής στην Ευρωπαϊκή Ένωση (ΕΕ) και παγκοσμίως.

- **Κακόβουλο λογισμικό**
  Το κακόβουλο λογισμικό είναι λογισμικό ή υλικολογισμικό που προορίζεται για την εκτέλεση μη εξουσιοδοτημένης διαδικασίας η οποία πρόκειται να έχει αρνητικές επιπτώσεις στην εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος. Η απειλή κακόβουλου λογισμικού κατατάσσεται σταθερά σε υψηλές θέσεις εδώ και πολλά χρόνια, αν και με μειούμενο ρυθμό κατά την περίοδο αναφοράς της έκθεσης ETL 2021. Η χρήση νέων τεχνικών σύναψης και ορισμένες σημαντικές νίκες της κοινότητας επιβολής του νόμου έχουν επηρεάσει τις επιχειρήσεις των σχετικών παραγόντων απειλής.

- **Cryptojacking (εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση)**
  Η εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση (cryptojacking ή cryptomining) είναι ένα είδος κυβερνοεγκλήματος στο πλαίσιο του οποίου οι εγκληματίες χρησιμοποιούν μυστικά την υπολογιστική ισχύ των θυμάτων για τη δημιουργία κρυπτονομίσματος. Μετά τον πολλαπλασιασμό των κρυπτονομισμάτων και την ολοένα αυξανόμενη αποδοχή τους από το ευρύτερο κοινό, παρατηρήθηκε αύξηση των αντίστοιχων περιστατικών κυβερνοασφάλειας.

- **Απειλές που σχετίζονται με το ηλεκτρονικό ταχυδρομείο**
  Οι επιθέσεις που σχετίζονται με το ηλεκτρονικό ταχυδρομείο είναι μια δέσμη απειλών οι οποίες, αντί για την τεχνική τρωτότητα των συστημάτων πληροφοριών, εκμεταλλεύονται τις αδυναμίες της ανθρώπινης ψυχής και των καθημερινών συνηθειών. Ενδιαφέρον προκαλεί το γεγονός ότι, παρά τις πολυάριθμες εκστρατείες ευαισθητοποίησης και εκπαίδευσης για την αντιμετώπιση αυτών των ειδών επιθέσεων, η απειλή εξακολουθεί να υφίσταται σε αξιοσημείωτο βαθμό. Ειδικότερα, βρίσκονται σε άνοδο η παραβίαση των επιχειρηματικών μηνυμάτων ηλεκτρονικού ταχυδρομείου και οι προηγμένες εξελιγμένες τεχνικές για την άντληση χρηματικού οφέλους.

- **Απειλές κατά των δεδομένων**
  Η κατηγορία αυτή περιλαμβάνει παραβιάσεις/διαρροές δεδομένων. Παραβίαση ή διαρροή δεδομένων είναι η δημοσιοποίηση ευαίσθητων, εμπιστευτικών ή προστατευόμενων δεδομένων σε μη αξιόπιστο περιβάλλον. Οι παραβιάσεις δεδομένων μπορεί να προκύψουν ως αποτέλεσμα κυβερνοεπίθεσης, εγκλήματος με συνεργία προσώπου που κατέχει προνομιακές πληροφορίες εκ των έσω, ακούσιας απώλειας ή έκθεσης δεδομένων. Η απειλή παραμένει υψηλή, δεδομένου ότι η πρόσβαση στα δεδομένα αποτελεί πρωταρχικό στόχο για τους επιτιθέμενους για πολλούς λόγους, π.χ. εκβίαση, λύτρα, δυσφήμιση, εσφαλμένη πληροφόρηση κ.λπ.

- **Απειλές κατά της διαθεσιμότητας και της ακεραιότητας**
  Η διαθεσιμότητα και η ακεραιότητα αποτελούν στόχο πληθώρας απειλών και επιθέσεων, μεταξύ των οποίων ξεχωρίζουν οι οικογένειες των επιθέσεων άρνησης υπηρεσίας (DoS) και των επιθέσεων σε ιστότοπους. Η DDoS συνδέεται αυστηρά με τις επιθέσεις μέσω διαδικτύου και αποτελεί μία από τις πλέον κρίσιμες απειλές για τα συστήματα ΤΠ, στοχεύοντας στη διαθεσιμότητά τους μέσω της εξάντλησης των πόρων, προκαλώντας μειώσεις στις επιδόσεις, απώλειες δεδομένων και διακοπές υπηρεσιών. Η απειλή κατατάσσεται σταθερά σε υψηλά επίπεδα στο τοπίο απειλών του ENISA, τόσο λόγω της εκδήλωσής της σε πραγματικά περιστατικά όσο και λόγω του δυναμικού της για υψηλό αντίκτυπο.

- **Παραπληροφόρηση – εσφαλμένη πληροφόρηση**
  Οι εκστρατείες παραπληροφόρησης και εσφαλμένης πληροφόρησης βρίσκονται σε άνοδο λόγω της αυξημένης χρήσης των πλατφορμών κοινωνικής δικτύωσης και των διαδικτυακών μέσων ενημέρωσης, καθώς και ως αποτέλεσμα της αύξησης της διαδικτυακής παρουσίας των ανθρώπων εξαιτίας της πανδημίας COVID-19. Η εν λόγω ομάδα απειλών εμφανίζεται για πρώτη φορά στην έκθεση ETL· ωστόσο, η σημασία της στον κυβερνοχώρο είναι υψηλή. Οι εκστρατείες παραπληροφόρησης και εσφαλμένης πληροφόρησης χρησιμοποιούνται συχνά σε υβριδικές επιθέσεις με σκοπό τη μείωση της συνολικής αντίληψης περί εμπιστοσύνης, η οποία αποτελεί μείζονα υπέρμαχο της κυβερνοασφάλειας.

- **Μη κακόβουλες απειλές**
  Οι απειλές θεωρούνται συνήθως οικειοθελείς και κακόβουλες δραστηριότητες αντιπάλων οι οποίοι έχουν ορισμένα κίνητρα να επιτεθούν σε συγκεκριμένο στόχο. Με την εν λόγω κατηγορία καλύπτουμε απειλές στις οποίες δεν είναι εμφανής η κακόβουλη πρόθεση. Αυτές βασίζονται κυρίως σε ανθρώπινα σφάλματα και σε εσφαλμένες ρυθμίσεις του συστήματος, ωστόσο μπορούν επίσης να αναφέρονται σε φυσικές καταστροφές που στοχεύουν υποδομές ΤΠ. Επίσης λόγω της φύσης τους, οι απειλές αυτές έχουν συνεχή παρουσία στο ετήσιο τοπίο των απειλών και αποτελούν μείζονα πηγή ανησυχίας για τις εκτιμήσεις κινδύνου.

Διάγραμμα 1: Τοπίο απειλών του ENISA για το 2021 - βασικές απειλές

Πρέπει να σημειωθεί ότι οι προαναφερθείσες απειλές αφορούν κατηγορίες και τη συλλογή απειλών οι οποίες ενοποιήθηκαν στους οκτώ προαναφερθέντες τομείς. Καθεμία από τις ομάδες απειλών αναλύεται περαιτέρω σε

ειδικό κεφάλαιο της παρούσας έκθεσης, το οποίο αναλύει τις ιδιαιτερότητες της ομάδας και παρέχει πιο συγκεκριμένες πληροφορίες, ευρήματα, τάσεις, τεχνικές επίθεσης και φορείς μετριασμού.

1.2. ΒΑΣΙΚΕΣ ΤΑΣΕΙΣ

Στον κατάλογο που ακολουθεί συνοψίζονται οι κύριες τάσεις που παρατηρήθηκαν στο τοπίο των απειλών στον κυβερνοχώρο κατά την περίοδο αναφοράς. Οι εν λόγω τάσεις εξετάζονται επίσης λεπτομερώς σε όλα τα διάφορα κεφάλαια που συνθέτουν το τοπίο απειλών του ENISA για το 2021.

- Όπως επισημαίνεται στην ειδική έκθεση του ENISA για το τοπίο απειλών στην αλυσίδα εφοδιασμού, οι **ιδιαίτερα εξελιγμένες και αποτελεσματικές παραβιάσεις σε αλυσίδες εφοδιασμού** έχουν πολλαπλασιαστεί. Οι **πάροχοι διαχειριζόμενων υπηρεσιών** αποτελούν για τους εγκληματίες του κυβερνοχώρου στόχους υψηλής αξίας.
- **Η νόσος COVID-19 υπήρξε παράγοντας ώθησης της κυβερνοκατασκοπείας** και δημιούργησε **ευκαιρίες για τους εγκληματίες του κυβερνοχώρου.**
- **Οι κυβερνητικοί οργανισμοί έχουν εντείνει τις προσπάθειές τους** σε εθνικό και διεθνές επίπεδο. Παρατηρήθηκε αύξηση των προσπαθειών των κυβερνήσεων για την εξάρθρωση και την ανάληψη νομικής δράσης κατά χρηματοδοτούμενων από το κράτος παραγόντων απειλών.
- **Οι εγκληματίες του κυβερνοχώρου υποκινούνται όλο και περισσότερο από τη χρηματοποίηση** των δραστηριοτήτων τους, π.χ. λυτρισμικό. Το **κρυπτονόμισμα** παραμένει η συνηθέστερη μέθοδος πληρωμής για τους παράγοντες απειλής.
- Οι επιθέσεις των εγκληματιών του κυβερνοχώρου **στοχεύουν και πλήττουν ολοένα και περισσότερο υποδομές ζωτικής σημασίας**.
- **Οι παραβιάσεις μέσω ηλεκτρονικών μηνυμάτων ηλεκτρονικού ψαρέματος (phishing) και οι επιθέσεις ωμής βίας σε υπηρεσίες απομακρυσμένης επιφάνειας εργασίας** παραμένουν οι δύο πλέον συνήθεις **φορείς μετάδοσης μόλυνσης από λυτρισμικό**.
- Η εστίαση στα **επιχειρηματικά μοντέλα τύπου Ransomware as a Service (RaaS)** αυξήθηκε κατά τη διάρκεια του 2021, καθιστώντας δύσκολη την ορθή κατανομή των μεμονωμένων παραγόντων απειλής.
- Κατά τη διάρκεια του 2021 σημείωσαν σημαντική αύξηση οι επιθέσεις **λυτρισμικού τριπλού εκβιασμού**.
- **Η μείωση του κακόβουλου λογισμικού** που παρατηρήθηκε το 2020 συνεχίζεται κατά τη διάρκεια του 2021. Το 2021 διαπιστώσαμε αύξηση των παραγόντων απειλής που καταφεύγουν σε σχετικά νέες ή ασυνήθιστες γλώσσες προγραμματισμού για τη μεταφορά του κώδικά τους.
- **Το κακόβουλο λογισμικό που στοχεύει περιβάλλοντα κοντέινερ** έχει καταστεί πολύ πιο διαδεδομένο, καθώς νέες εξελίξεις, όπως το κακόβουλο λογισμικό χωρίς τη χρήση αρχείων, εκτελούνται από τη μνήμη.
- Οι κατασκευαστές κακόβουλου λογισμικού συνεχίζουν να βρίσκουν τρόπους για να **καθιστούν πιο δύσκολη την ανάδρομη τεχνική έρευνα και τη δυναμική ανάλυση.**
- Σε σύγκριση με τα τελευταία έτη, το πρώτο τρίμηνο του 2021 ο αριθμός **μολύνσεων από λογισμικό cryptojacking** κατέγραψε **πρωτοφανές υψηλό επίπεδο**. Το **οικονομικό όφελος** που συνδέεται με την εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση παρείχε κίνητρα στους παράγοντες απειλής για την πραγματοποίηση των εν λόγω επιθέσεων.
- **Ο αριθμός δραστηριοτήτων cryptomining και cryptojacking το 2021 βρίσκεται σε πρωτοφανή υψηλά επίπεδα**.
- Διαπιστώνουμε ότι βρίσκεται σε εξέλιξη μια **μετάβαση από την εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση μέσω προγράμματος περιήγησης στην εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση με χρήση αρχείων**.
- **Η νόσος COVID-19 εξακολουθεί να αποτελεί το κυρίαρχο δόλωμα στις εκστρατείες** επιθέσεων ηλεκτρονικού ταχυδρομείου.
- Οι **παραβιάσεις επιχειρηματικών διευθύνσεων ηλεκτρονικού ταχυδρομείου** έχουν **αυξηθεί**, έχουν αναπτυχθεί σε επίπεδο **πολυπλοκότητας** και έχουν γίνει πιο **στοχευμένες**.
- Το επιχειρηματικό μοντέλο **Phishing-as-a-Service (PhaaS)** κερδίζει έδαφος.
- Οι παράγοντες απειλής μετατόπισαν το επίκεντρο της προσοχής τους στις **πληροφορίες σχετικά με τα εμβόλια** στο πλαίσιο απειλών κατά των δεδομένων και των πληροφοριών.
- Σημειώθηκε **απότομη αύξηση των παραβιάσεων δεδομένων που σχετίζονται με τον τομέα της υγειονομικής περίθαλψης**.

- Οι παραδοσιακές επιθέσεις DDoS (Distributed Denial of Service-κατανεμημένης επίθεσης άρνησης υπηρεσίας) μετατοπίζονται προς τα **δίκτυα κινητής τηλεφωνίας και το ΔτΠ (διαδίκτυο των πραγμάτων).**
- Το **Ransom Denial of Service (RDoS)** είναι η νέα πρόκληση των επιθέσεων άρνησης υπηρεσίας.
- **Η κοινή χρήση πόρων σε εικονικά περιβάλλοντα** λειτουργεί ως παράγοντας ενίσχυσης των επιθέσεων DDoS.
- **Οι εκστρατείες DDoS** το 2021 έχουν γίνει πιο στοχευμένες και πολύ πιο επίμονες και με ολοένα και περισσότερους πολλαπλούς φορείς επίθεσης.
- **Η παραπληροφόρηση που βασίζεται στην τεχνητή νοημοσύνη (ΤΝ)** υποστηρίζει τους επιτιθέμενους κατά τη διάρκεια των επιθέσεων.
- **Το ηλεκτρονικό «ψάρεμα» βρίσκεται στο επίκεντρο των επιθέσεων παραπληροφόρησης** και αξιοποιεί σε μεγάλο βαθμό τις πεποιθήσεις των πολιτών.
- **Η παραπληροφόρηση και η εσφαλμένη πληροφόρηση** βρίσκονται στο επίκεντρο των δραστηριοτήτων κυβερνοεγκλήματος και αυξάνονται με πρωτοφανή ρυθμό.
- **Το επιχειρηματικό μοντέλο Disinformation-as-a-Service (DaaS - παραπληροφόρηση ως υπηρεσία)** αυξήθηκε σημαντικά, λόγω του αυξανόμενου αντικτύπου της πανδημίας COVID-19 και της ανάγκης για περισσότερες πληροφορίες.
- Το 2020 και το 2021 παρατηρήσαμε **απότομη αύξηση των μη κακόβουλων περιστατικών**, καθώς η πανδημία COVID-19 κατέστη πολλαπλασιαστής των **ανθρωπίνων σφαλμάτων** και των **εσφαλμένων ρυθμίσεων συστήματος**, σε σημείο που οι περισσότερες παραβάσεις το 2020 προκλήθηκαν από σφάλματα.
- Σημειώθηκε **απότομη αύξηση των μη κακόβουλων περιστατικών ασφάλειας υπολογιστικού νέφους**.

1.3. ΕΓΓΥΤΗΤΑ ΤΩΝ ΚΥΡΙΟΤΕΡΩΝ ΑΠΕΙΛΩΝ ΣΤΗΝ ΕΕ

Σημαντική πτυχή η οποία πρέπει να εξεταστεί στο πλαίσιο του τοπίου απειλών του ENISA είναι η εγγύτητα μιας κυβερνοαπειλής σε σχέση με την Ευρωπαϊκή Ένωση (ΕΕ). Αυτό είναι ιδιαίτερα σημαντικό για την παροχή βοήθειας στους αναλυτές κατά την αξιολόγηση της σημασίας των κυβερνοαπειλών, τη συσχέτισή τους με δυνητικούς παράγοντες απειλής και φορείς, καθώς και για την καθοδήγηση της επιλογής κατάλληλων στοχοθετημένων φορέων μετριασμού. Σύμφωνα με την προτεινόμενη ταξινόμηση για την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ) της ΕΕ[7], ταξινομούμε τις κυβερνοαπειλές σε τέσσερις κατηγορίες, όπως απεικονίζεται στον **Πίνακας 1**.

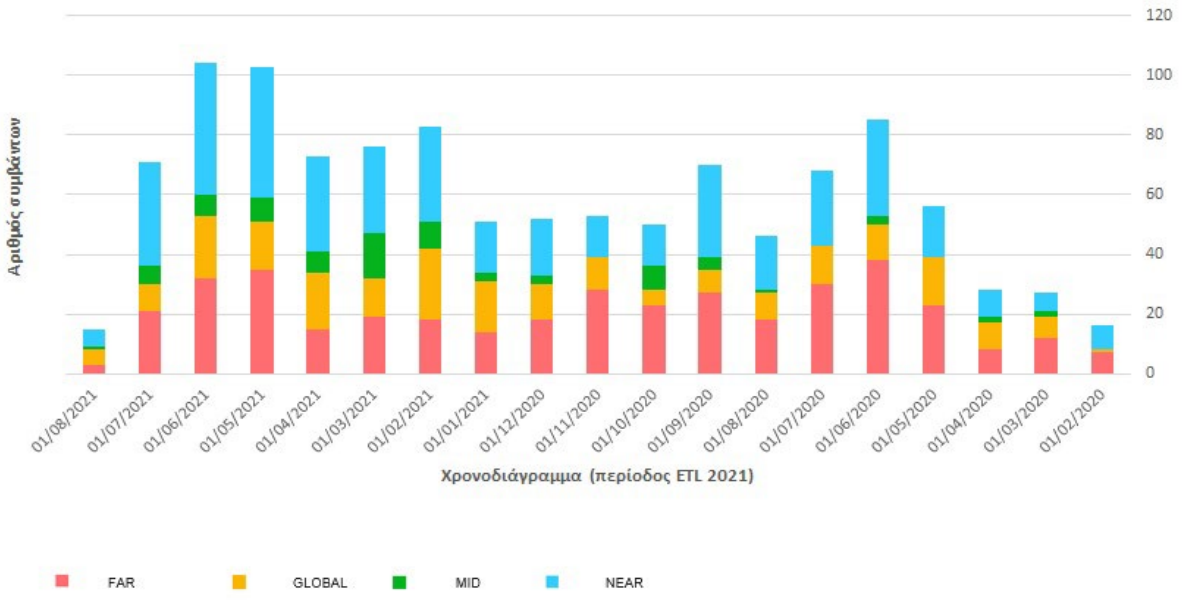
Πίνακας 1: Ταξινόμηση της εγγύτητας των κυβερνοαπειλών

Εγγύτητα	Ανησυχίες
NEAR	Πληττόμενα δίκτυα, συστήματα, ελεγχόμενα και διασφαλισμένα εντός των συνόρων της ΕΕ. Πληττόμενος πληθυσμός εντός των συνόρων της ΕΕ.
MID	Δίκτυα και συστήματα τα οποία θεωρούνται ζωτικής σημασίας για επιχειρησιακούς στόχους εντός του πεδίου εφαρμογής της ψηφιακής ενιαίας αγοράς της ΕΕ και των τομέων της οδηγίας NIS, των οποίων ωστόσο ο έλεγχος και η διασφάλιση εξαρτώνται από θεσμικές αρχές εκτός ΕΕ ή δημόσιες ή ιδιωτικές αρχές των κρατών μελών. Πληττόμενος πληθυσμός σε γεωγραφικές περιοχές κοντά στα σύνορα της ΕΕ.
FAR	Δίκτυα και συστήματα τα οποία, εάν επηρεαστούν, θα έχουν κρίσιμο αντίκτυπο στους επιχειρησιακούς στόχους εντός του πεδίου εφαρμογής της ψηφιακής ενιαίας αγοράς της ΕΕ και των τομέων της οδηγίας NIS. Ο έλεγχος και η διασφάλιση των εν λόγω δικτύων και συστημάτων εξαρτάται από φορείς πέραν των θεσμικών αρχών της ΕΕ ή των δημόσιων ή ιδιωτικών αρχών των κρατών μελών της ΕΕ. Πληττόμενος πληθυσμός σε γεωγραφικές περιοχές μακριά από την ΕΕ.
GLOBAL	Όλες οι προαναφερθείσες περιοχές

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Το Διάγραμμα 2 παρουσιάζει ένα χρονοδιάγραμμα περιστατικών τα οποία σχετίζονται με τις βασικές κατηγορίες απειλών που αναφέρονται στην έκθεση ETL 2021. Θα πρέπει να σημειωθεί ότι οι πληροφορίες του γραφήματος βασίζονται σε πληροφορίες ανοικτής πηγής και είναι αποτέλεσμα των εργασιών του ENISA στον τομέα της επίγνωσης της κατάστασης[8].

Διάγραμμα 2: Χρονοδιάγραμμα των παρατηρούμενων περιστατικών που σχετίζονται με μείζονες απειλές στο πλαίσιο της έκθεσης ETL (επίγνωση της κατάστασης βάσει πληροφοριών ανοικτής πηγής) όσον αφορά την εγγύτητά τους.



Όπως αποδεικνύεται από το παραπάνω διάγραμμα, το 2021 σημειώθηκε μεγαλύτερος αριθμός συμβάντων σε σύγκριση με το 2020. Ειδικότερα, η κατηγορία NEAR παρουσιάζει έναν διαρκώς αυξανόμενο αριθμό παρατηρούμενων περιστατικών τα οποία σχετίζονται με βασικές απειλές, γεγονός που καταδεικνύει τη σημασία τους στο πλαίσιο της ΕΕ. Δεν προκαλεί έκπληξη το γεγονός ότι οι μηνιαίες τάσεις (οι οποίες για λόγους συντομίας δεν εμφανίζονται στο διάγραμμα) είναι αρκετά παρόμοιες μεταξύ των διαφορετικών ταξινομήσεων, δεδομένου ότι η κυβερνοασφάλεια δεν γνωρίζει σύνορα και, στις περισσότερες περιπτώσεις, οι απειλές υλοποιούνται σε όλα τα επίπεδα εγγύτητας. Αξίζει να σημειωθεί ότι, κατά τη διάρκεια των τελευταίων μηνών τους οποίους καλύπτει η έκθεση ETL 2021, παρατηρείται μεγαλύτερη εγγύτητα της ΕΕ στο πλαίσιο της NEAR, τάση την οποία ο ENISA θα συνεχίσει να παρακολουθεί για να διαπιστώσει πώς εξελίσσεται και πώς συνδέεται με τις δραστηριότητες των παραγόντων απειλής και των συνεχιζόμενων φορέων απειλής.

1.4. ΒΑΣΙΚΕΣ ΑΠΕΙΛΕΣ ΑΝΑ ΤΟΜΕΑ

Οι κυβερνοαπειλές συνήθως δεν περιορίζονται σε συγκεκριμένο τομέα και στις περισσότερες περιπτώσεις επηρεάζουν περισσότερους από έναν εξ αυτών. Αυτό ισχύει πράγματι, δεδομένου ότι σε πολλές περιπτώσεις οι απειλές εκδηλώνονται με την εκμετάλλευση της τρωτότητας των υποκείμενων συστημάτων ΤΠΕ που χρησιμοποιούνται σε διάφορους τομείς. Ωστόσο, οι στοχευμένες επιθέσεις, καθώς και οι επιθέσεις που εκμεταλλεύονται τις διαφορές όσον αφορά την ωριμότητα στον τομέα της κυβερνοασφάλειας σε όλους τους τομείς και τη δημοτικότητα/προβολή ορισμένων τομέων, αποτελούν παράγοντες που πρέπει να ληφθούν υπόψη. Οι παράγοντες αυτοί συμβάλλουν στην εκδήλωση των απειλών ως περιστατικών κυβερνοασφάλειας σε

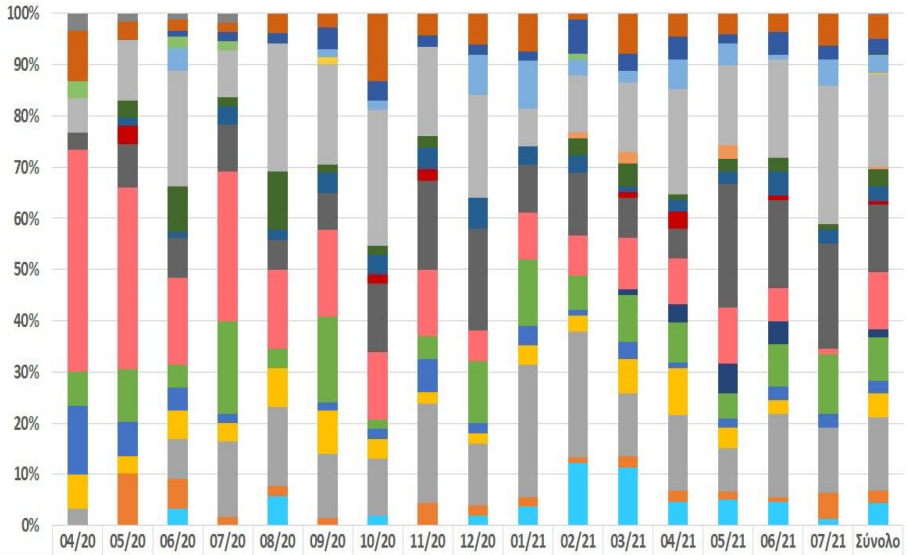
[8] Σύμφωνα με το άρθρο 7 παράγραφος 6 της πράξης για την κυβερνοασφάλεια της ΕΕ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

συγκεκριμένους τομείς και αυτός είναι ο λόγος για τον οποίο είναι σημαντικό να εξεταστούν ενδελεχώς οι τομεακές πτυχές των παρατηρούμενων περιστατικών και απειλών. Επιπλέον, μέσα από μια ανάλυση αυτού του είδους είναι δυνατή η άντληση τάσεων που παρατηρούνται σε κάθε τομέα και σε διατομεακές εξαρτήσεις.

Το διάγραμμα 3 και το διάγραμμα 4 επισημαίνουν τους πληττόμενους τομείς σχετικά με περιστατικά κυβερνοασφάλειας που παρατηρήθηκαν με βάση πληροφορίες ανοικτής πηγής και είναι αποτέλεσμα των εργασιών του ENISA στον τομέα της επίγνωσης της κατάστασης[9]. Αναφέρονται σε περιστατικά που σχετίζονται με τις βασικές απειλές της έκθεσης ETL 2021. Πρόκειται για την πρώτη προσπάθεια του ENISA να χαρτογραφήσει τον αντίκτυπο των απειλών σε συγκεκριμένους τομείς. Τα επόμενα έτη και στις μελλοντικές εκδόσεις του τοπίου των απειλών, θα καταβληθούν προσπάθειες για την ευθυγράμμιση των τομέων με εκείνους που απαριθμούνται στην οδηγία για την ασφάλεια δικτύων και πληροφοριών (οδηγία NIS) και στην πρόταση για την αναθεώρησή της (οδηγία NIS 2.0).

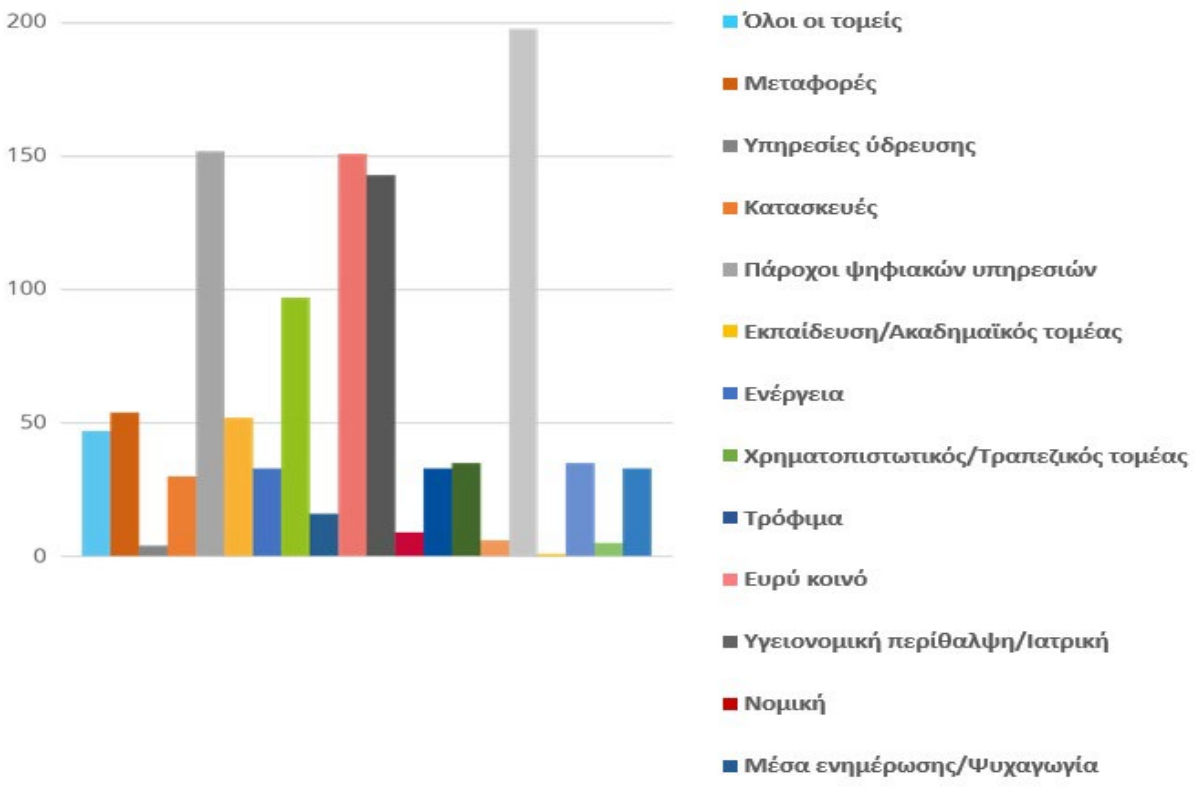
[9] Σύμφωνα με το άρθρο 7 παράγραφος 6 της πράξης για την κυβερνοασφάλεια της ΕΕ (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Διάγραμμα 3: Χρονοδιάγραμμα των παρατηρούμενων περιστατικών που σχετίζονται με βασικές απειλές στο πλαίσιο της έκθεσης ETL όσον αφορά τον πληττόμενο τομέα.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Σύνολο
Υπηρεσίες ύδρευσης	1	1	1	1													2
Μεταφορές	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Στοχευόμενα άτομα			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Διάστημα	1		2	1							1						4
Αλυσίδα εφοδιασμού λογισμικού			4			1	1		4	5	3	2	5	5	1	4	35
Ημιαγωγοί						1											1
Δημόσια διοίκηση/Κυβέρνηση	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών											1	2		3			6
Στρατός		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Μέσα ενημέρωσης/Ψυχαγωγία		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Νομική		2					1	1				1	3		1		7
Υγειονομική περίθαλψη/Ιατρική	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Ευρύ κοινό	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Τρόφιμα												1	3	7	5		16
Χρηματοπιστωτικός/Τραπεζικός τομέας	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Ενέργεια	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Εκπαίδευση/Ακαδημαϊκός τομέας	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Πάροχοι ψηφιακών υπηρεσιών	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Κατασκευές		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Όλοι οι τομείς			3		3		1		1	2	11	10	4	6	5	1	47

Διάγραμμα 4: Στοχευμένοι τομείς ανά αριθμό περιστατικών (Απρίλιος 2020 - Ιούλιος 2021)



Κατά τη διάρκεια της εν λόγω περιόδου αναφοράς, μεγάλος αριθμός περιστατικών είχε ως στόχο φορείς δημόσιας διοίκησης, κυβερνητικούς φορείς και παρόχους ψηφιακών υπηρεσιών. Για τους τελευταίους αυτό είναι αναμενόμενο, λόγω της οριζόντιας παροχής υπηρεσιών για τον εν λόγω τομέα και, ως εκ τούτου, του αντικτύπου της σε πολλούς άλλους τομείς. Παρατηρήσαμε επίσης μεγάλο αριθμό περιστατικών που στόχευαν τους τελικούς χρήστες και όχι απαραίτητα κάποιον συγκεκριμένο τομέα. Ο τομέας της υγείας στοχεύθηκε σε εξίσου μεγάλο βαθμό και η δραστηριότητα αυτή παρουσιάζει ενδείξεις αύξησης κατά τους τελευταίους μήνες της περιόδου αναφοράς (Μάιος-Ιούλιος 2021). Ενδιαφέρον παρουσιάζει το γεγονός ότι ο χρηματοπιστωτικός τομέας αντιμετωπίζει συνεπή αριθμό περιστατικών καθ' όλη τη διάρκεια του έτους. Η αλυσίδα εφοδιασμού λογισμικού δείχνει επίσης αυξημένο αριθμό περιστατικών κατά τη διάρκεια του 2021, γεγονός που βρίσκεται ως παρατήρηση και στην έκθεση του ENISA για το τοπίο των απειλών στην αλυσίδα εφοδιασμού[10].

1.5. ΜΕΘΟΔΟΛΟΓΙΑ

Η έκθεση του ENISA για το τοπίο των απειλών (ETL) για το 2021 βασίζεται σε πληροφορίες οι οποίες είναι διαθέσιμες από ανοικτές πηγές, κυρίως στρατηγικού χαρακτήρα, και στις ικανότητες συλλογής πληροφοριών για τις κυβερνοαπειλές (CTI) του ίδιου του ENISA, και καλύπτει περισσότερους από έναν τομείς, τεχνολογίες και πλαίσια. Η έκθεση επιχειρεί να τηρήσει «αγνωστικιστική» στάση όσον αφορά τα δεδομένα της βιομηχανίας και των κατασκευαστών και περιέχει, σε πολλές υποσημειώσεις μέσα στο κείμενο, βιβλιογραφικές αναφορές ή παραπομπές σε έργα διαφόρων ερευνητών στον τομέα της ασφάλειας, ιστολογίων ασφαλείας και άρθρων ειδησεογραφικών μέσων. Η έκθεση ETL 2021 καλύπτει το χρονικό διάστημα από τον Απρίλιο του 2020 έως τον Ιούλιο του 2021 το οποίο αναφέρεται σε όλη την έκθεση ως «περίοδος αναφοράς» .

Για την κατάρτιση της έκθεσης ETL 2021 χρησιμοποιήθηκε η ακόλουθη προσέγγιση. Καθ' όλη τη διάρκεια της σχετικής χρονικής περιόδου, ο ENISA συγκέντρωσε με τη χρήση μέσων επίγνωσης της κατάστασης κατάλογο σημαντικών περιστατικών όπως αυτά εμφανίστηκαν σε ανοικτές πηγές. Ο κατάλογος αυτός χρησίμευσε ως βάση για

[10] ENISA Threat Landscape for Supply Chain Attacks, Ιούλιος 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

τον προσδιορισμό του καταλόγου των βασικών απειλών, καθώς και του βασικού υλικού για διάφορες τάσεις και στατιστικά στοιχεία της έκθεσης.

Στη συνέχεια, ο ENISA και εξωτερικοί εμπειρογνώμονες διεξήγαγαν διεξοδική έρευνα τεκμηρίωσης της διαθέσιμης βιβλιογραφίας από ανοικτές πηγές, όπως άρθρα ειδησεογραφικών μέσων, γνωμοδοτήσεις εμπειρογνωμόνων, εκθέσεις πληροφοριών, αναλύσεις συμβάντων και ερευνητικές εκθέσεις σχετικά με την ασφάλεια. Μέσω συνεχούς ανάλυσης, ο ENISA προέβη στην εξαγωγή τάσεων και σημείων ενδιαφέροντος για καθεμία από τις μείζονες απειλές που παρουσιάζονται στην έκθεση ETL 2021. Τα βασικά πορίσματα και οι διαπιστώσεις της παρούσας αξιολόγησης βασίζονται σε πολλαπλούς και δημόσια διαθέσιμους πόρους, οι οποίοι παρέχονται στις βιβλιογραφικές πηγές που χρησιμοποιήθηκαν για την κατάρτιση του παρόντος εγγράφου.

Εντός της έκθεσης, επιδιώκουμε να διαφοροποιούμε τη στάση μας όσον αφορά τη σχέση των στοιχείων που αναφέρθηκαν από τις πηγές μας με την αξιολόγησή μας. (Αυτό γίνεται με τη χρήση ειδικά της φράσης «κατά την αξιολόγησή μας»). Τέλος, κατά τη διενέργεια αξιολόγησης, χρησιμοποιούνται λέξεις που εκφράζουν εκτίμηση της πιθανότητας (π.χ. πιθανόν, πολύ πιθανόν, σίγουρα)[11].

Στην παρούσα έκθεση χρησιμοποιήθηκε το πλαίσιο MITRE ATT&CK®[12] για την επισήμανση των τακτικών και των τεχνικών επίθεσης που σχετίζονται με δεδομένη απειλή (βλέπε παράρτημα Α). Για κάθε τακτική ATT&CK® παρουσιάζονται οι τεχνικές που χρησιμοποίησαν οι αντίπαλοι. Αυτό μπορεί να οδηγήσει σε έναν κατάλογο λύσεων μετριασμού των επιθέσεων οι οποίες είναι δυνατόν να εφαρμόζονται με βάση το πλαίσιο MITRE ATT&CK[13] . Το MITRE ATT&CK® είναι μια γνωσιακή βάση που περιέχει μια κοινή γλώσσα για τις τακτικές των αντιπάλων και τις τεχνικές και βασίζεται σε παρατηρήσεις υπό πραγματικές συνθήκες. Η βάση γνώσεων MITRE ATT&CK® χρησιμοποιείται ως βάση για την ανάπτυξη συγκεκριμένων μοντέλων απειλών και μεθοδολογιών στον ιδιωτικό τομέα, στην κυβέρνηση και στην κοινότητα προϊόντων και υπηρεσιών κυβερνοασφάλειας.

Η έκθεση επικυρώθηκε από την ad hoc ομάδα εργασίας του ENISA για τα τοπία απειλών στον κυβερνοχώρο[14] η οποία συστάθηκε τον Απρίλιο του 2021, μια ομάδα αποτελούμενη από εμπειρογνώμονες από ευρωπαϊκές και διεθνείς οντότητες του δημόσιου και του ιδιωτικού τομέα.

Όσον αφορά τη μελλοντική ανάπτυξη εκθέσεων Τοπίων Απειλών, ο ENISA βρίσκεται στο στάδιο της επισημοποίησης μιας νέας μεθοδολογίας, προκειμένου να προωθήσει τη διαφάνεια και να θέσει τα θεμέλια για δομημένες και καλά ευθυγραμμισμένες διαδικασίες. Στο πλαίσιο αυτής της προσπάθειας, σε συνδυασμό με μια αναθεώρηση της ταξινόμησης των απειλών, πρόκειται να δημοσιοποιηθεί μελλοντικά η μεθοδολογία για τα τοπία των απειλών.

1.6. ΔΙΑΡΘΡΩΣΗ ΤΗΣ ΕΚΘΕΣΗΣ

Το έκθεση του ENISA για το τοπίο των απειλών (ETL) για το 2021 διατήρησε τη διάρθρωση των προηγούμενων εκθέσεων ETL χρησιμοποιώντας παρόμοια διάρθρωση για την ανάδειξη των βασικών κυβερνοαπειλών το 2021. Οι αναγνώστες παλαιότερων εκδόσεων θα διαπιστώσουν ότι οι κατηγορίες απειλών έχουν ενοποιηθεί σύμφωνα με μια μετάβαση προς μια νέα ταξινόμηση των απειλών για την κυβερνοασφάλεια η οποία πρόκειται να χρησιμοποιηθεί μελλοντικά.

Η παρούσα έκθεση διαρθρώνεται ως εξής:

Το **κεφάλαιο 2** διερευνά τις τάσεις που σχετίζονται με τους παράγοντες απειλής (δηλ. τους χρηματοδοτούμενους από το κράτος παράγοντες, τους παράγοντες κυβερνοεγκλήματος, τους χάκερ που προσφέρουν τις υπηρεσίες τους επ' αμοιβή και τους χακτιβιστές).
Στο **κεφάλαιο 3** εξετάζονται σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά το λυτρισμικό.
Στο **κεφάλαιο 4** παρουσιάζονται σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά το κακόβουλο λογισμικό.

[11] CIA - Words of Estimative Probability https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

Στο **κεφάλαιο 5** περιγράφονται σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά την εξόρυξη κρυπτονομισμάτων χωρίς εξουσιοδότηση (cryptojacking).
Στο **κεφάλαιο 6** επισημαίνονται σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά απειλές που σχετίζονται με το ηλεκτρονικό ταχυδρομείο.
Στο **κεφάλαιο 7** εξετάζονται σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά τις απειλές κατά των δεδομένων.
Στο **κεφάλαιο 8** παρουσιάζονται σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά τις απειλές κατά της διαθεσιμότητας και της ακεραιότητας.
Στο **κεφάλαιο 9** υπογραμμίζεται η σημασία των υβριδικών απειλών και περιγράφονται σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά την παραπληροφόρηση και την εσφαλμένη πληροφόρηση.
Το **κεφάλαιο 10** επικεντρώνεται σε σημαντικά ευρήματα, περιστατικά και τάσεις όσον αφορά τις μη κακόβουλες απειλές.
Στο **παράρτημα Α** παρουσιάζονται οι τεχνικές που χρησιμοποιούνται συνήθως για κάθε απειλή, με βάση το πλαίσιο MITRE ATT&CK®.
Το **παράρτημα Β** περιλαμβάνει αξιοσημείωτα συμβάντα ανά απειλή, όπως παρατηρήθηκαν κατά την περίοδο αναφοράς.