

Θέμα: Δημιουργία Πλατφόρμας για την ανίχνευση και αντιμετώπιση κυβερνοεπιθέσεων με χρήση NLP, AI και Νευρωνικών Δικτύων	
Επιβλέπων: Β. Ταμπακάς	e-mail: tampakas@uop.gr
Μέλη:	Ακαδημαϊκό Έτος: 2024-25
Στόχοι Η εργασία αυτή στοχεύει στη δημιουργία ενός εργαλείου που θα συνδυάζει τεχνολογίες νευρωνικών δικτύων και επεξεργασίας φυσικής γλώσσας (NLP) για την ανάλυση και πρόβλεψη απειλών στο Dark Web	
Αντικείμενο Το εργαλείο θα συλλέγει και θα αναλύει δεδομένα από forums και marketplaces του Dark Web, με στόχο την ανίχνευση κακόβουλων μοτίβων και την πρόβλεψη μελλοντικών επιθέσεων σε πραγματικό χρόνο. Η Generative AI θα χρησιμοποιηθεί για τη δημιουργία προγνωστικών σεναρίων, παρέχοντας τη δυνατότητα ανίχνευσης απειλών πριν αυτές πραγματοποιηθούν. Το εργαλείο θα ενισχύσει την ικανότητα των οργανισμών να αντιδρούν σε νέες μορφές επιθέσεων και θα συμβάλει στη βελτίωση της κυβερνοασφάλειας.	
Αναφορές: Dark Web Activity Classification Using Deep Learning Αυτή η έρευνα εστιάζει στην ανάλυση δραστηριοτήτων του Dark Web χρησιμοποιώντας τεχνικές deep learning. Το εργαλείο ταξινομεί δραστηριότητες όπως το εμπόριο ναρκωτικών και όπλων, ανιχνεύοντας τίτλους και λέξεις-κλειδιά από ιστοσελίδες με κατάληξη ".onion". Προτείνει μια μέθοδο ταξινόμησης που βασίζεται στην εξαγωγή εικόνων και κειμένων από τον σκοτεινό ιστό και επιτυγχάνει ακρίβεια 94% στο σύνολο δεδομένων που χρησιμοποιήθηκε. (https://arxiv.org/abs/2306.07980) Dark Side of the Web: Dark Web Classification Based on Cyber Threats Αυτή η μελέτη εστιάζει στην κατηγοριοποίηση των απειλών που προέρχονται από το Dark Web χρησιμοποιώντας NLP και νευρωνικά δίκτυα. Αναλύει κακόβουλες δραστηριότητες, όπως η πώληση παράνομων προϊόντων και η κλοπή δεδομένων, και προτείνει ένα σύστημα κατηγοριοποίησης που συμβάλλει στην πρόληψη κυβερνοεπιθέσεων. Το σύστημα χρησιμοποιεί ανάλυση μεγάλων όγκων δεδομένων για να εντοπίσει επικίνδυνες δραστηριότητες και να βελτιώσει την ανίχνευση κυβερνοαπειλών. (https://ieeexplore.ieee.org/document/9266622) A Generative Adversarial Learning Framework for Breaking Text-Based CAPTCHA in the Dark Web Αυτή η έρευνα προτείνει τη χρήση γεννητικών αντιπαραθετικών δικτύων (GANs) για την ανάλυση και σπάσιμο text-based CAPTCHA στο Dark Web. Το CAPTCHA χρησιμοποιείται συχνά για την αποτροπή συλλογής δεδομένων στο	

Dark Web, και η μελέτη αυτή εξετάζει πώς μπορούν να παρακαμφθούν αυτά τα συστήματα με τη χρήση GANs.

(<https://ieeexplore.ieee.org/document/9280537>)

Η εργασία περιλαμβάνει:

Μελέτη Βιβλιογραφίας και Εξοικείωση με το Αντικείμενο

Εξόρυξη Δεδομένων:

Ανάπτυξη Μοντέλου, Σχεδιασμός συστήματος και υλοποίηση

Αξιολόγηση:.