ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΟ ΣΠΟΥΔΩΝ - ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μεταϋπολογισμός βαθμού επικινδυνότητας IP και URL διευθύνσεων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΡΙΖΙΚΟΥ ΙΩΑΝΝΗ

Επιβλέποντες: Μπαρμπάτσαλου Κωνσταντία

Καμπουράκης Γεώργιος

Μέλη της εξεταστικής επιτροπής: Καμπουράκης Γεώργιος

Καρύδα Μαρία

ΣΑΜΟΣ

ΜΑΡΤΙΟΣ 2021

Ευχαριστίες

Η παρούσα εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος «ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ» υπό την επίβλεψη της διδάσκουσας καθηγήτριας κ.Μπαρμπάτσαλου Κωνσταντίας και του καθηγητή κ.Καμπουράκη Γεωργίου. Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τη διδάσκουσα τόσο για την ανάθεση του θέματος, όσο και για την καθοδήγησή της στην πορεία της εργασίας.

Abstract

As we enter the new Digital era, the Internet is constantly growing, providing new innovative services. Even though these services are developed in order to facilitate everyday tasks and promote communication without borders, they are exploited by certain groups of people that aim to disrupt their confidentiality, integrity and availability features. The aforementioned groups take advantage of the scalable, distributed, and rather easily accessible naming, hosting and routing infrastructures of the Internet. As a result, the battle against malware is raging on multiple fronts: the endpoints, the network perimeter, and the application layer. The need for efficient and drastic measures so as to gain advantages against the various malicious entities, has never been greater.

For the purpose of this dissertation, a mobile application, aiming to detect and evaluate the reputation of Domain/IP addresses using the api of different detection and analysis tools such as VirusTotal, XFE and AbuseIPDB has been developed.

The three searching tools, mentioned above, extract a separate score indicating the maliciousness level of the registered address by the user. Apart from that, the user can also access and edit the responses of each individual api, while navigating through the history tab and has the ability to receive detailed information about current and previous results.

Moreover, the current dissertation provides historical data regarding the most significant and notorious internet attacks, general definitions and reporting of malicious content hosted on IPs / Urls and analysis of the various cyber-attacks types and their impact. As the need for protection is continuously rising, the usage of APIs in security is presented as a measure against malicious attacks. The API is the interface that gives the user immediate and prompt access to the required information provided by the analysis tools.

Apart from the above, three malware detection systems that were used in the current application and the methodology through the analysis of the results are presented.

Περίληψη

Καθώς εισερχόμαστε όλο και πιο βαθιά στην ψηφιακή εποχή, το Διαδίκτυο διαρκώς εξελίσσεται, παρέχοντας νέες καινοτόμες υπηρεσίες. Παρόλο που αυτές οι υπηρεσίες έχουν αναπτυχθεί για να διευκολύνουν τις καθημερινές ανάγκες προωθώντας την χωρίς σύνορα επικοινωνία, τυγχάνουν εκμετάλλευσης από ορισμένες ομάδες ανθρώπων που σκοπό έχουν να πλήξουν τα χαρακτηριστικά εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας αυτών των υπηρεσιών.

Κακόβουλοι χρήστες, εκμεταλλευόμενοι τις ευπάθειες τόσο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και τις αδυναμίες των χρηστών προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, επιχειρώντας να αποκομίσουν κέρδος ή να επηρεάσουν κακοβούλως την λειτουργία των συστημάτων. Συνεπώς η ανάγκη για αποτελεσματικά και δραστικά μέτρα έναντι των διαφόρων κακόβουλων οντοτήτων, δεν υπήρξε ποτέ μεγαλύτερη.

Για τους σκοπούς αυτής της διατριβής, έχει αναπτυχθεί μια εφαρμογή για συσκευές κινητής τηλεφωνίας, που έχει ώς στόχο την ανίχνευση και αξιολόγηση της φήμης των διευθύνσεων Url/ IP χρησιμοποιώντας το API διαφορετικών εργαλείων σάρωσης και ανίχνευσης κακόβουλου λογισμικού όπως το VirusTotal, XFE και AbuseIPDB.

Τα τρία εργαλεία αναζήτησης, που αναφέρθηκαν παραπάνω, εξάγουν μια ξεχωριστή βαθμολογία που δείχνει το επίπεδο επικινδυνότητας της καταχωρημένης από τον χρήστη διεύθυνσης Ip η Url. Ο χρήστης μπορεί επίσης να έχει πρόσβαση και να επεξεργάζεται τις απαντήσεις κάθε μεμονωμένου API, ενώ πλοηγείτε στην καρτέλα ιστορικό ενώ ταυτόχρονα έχει τη δυνατότητα να λαμβάνει λεπτομερείς πληροφορίες σχετικά με τα τρέχοντα και τα προηγούμενα αποτελέσματα.

Επιπλέον, η τρέχουσα διατριβή παρέχει στοιχεία σχετικά με τις σημαντικότερες διαδικτυακές επιθέσεις και τις επιπτώσεις αυτών καθώς και γενικούς ορισμούς και αναφοράς κακόβουλου περιεχομένου που φιλοξενείται σε Ip/Url, ενώ παρέχονται πληροφορίες και σχετικά με την API τεχνολογία και την συνεισφορά της στην άμεση μετάδοση πληροφοριών για την ανίχνευση και η ανάλυση του κακόβουλου λογισμικού.

Τέλος, πέρα από τα παραπάνω, παρουσιάζονται τρείς μηχανές ανίχνευσης κακόβουλου λογισμικού που χρησιμοποιήθηκαν στην τρέχουσα εφαρμογή ενώ παρουσιάζονται ενδεικτικά παραδείγματα από τη χρήση της εφαρμογής.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

1. Εισαγωγή

Τα τελευταία χρόνια, η θέση που έχει το διαδίκτυο στη ζωή, είναι πολύ σημαντική και αισθητά αυξημένη σε σχέση με τη θέση που είχε μια δεκαετία πριν. Το διαδίκτυο είναι ένας παγκόσμιος ιστός, που συνδέει ιδιώτες και επιχειρήσεις σε ολόκληρο τον κόσμο. Το μεγαλύτερο μέρος της επιτυχίας του το οφείλει στο γεγονός ότι επιτρέπει την εύκολη και με χαμηλό κόστος πρόσβαση και χρήση των υπηρεσιών του. Η αρχιτεκτονική του διαδικτύου είναι πράγματι μοναδική, καθώς είναι αποκεντρωμένο, χωρίς καμία εξάρτηση από κάποιο κεντρικό σύστημα διανομής και χρησιμοποιεί μία τεχνολογία μεταγωγής πακέτων, η οποία δεν μπορεί να ελεγχθεί από τους παραδοσιακούς μηχανισμούς που χρησιμοποιούνται στον τομέα των τηλεπικοινωνιών.

Το διαδίκτυο πλέον αποτελεί το κατ' εξοχήν εργαλείο αναζήτησης δεδομένων, παρέχει απίστευτες δυνατότητες για αναζήτηση πληροφοριών, ενημέρωση, ψυχαγωγία, επικοινωνία και κοινωνική δικτύωση, μάθηση, ηλεκτρονικές υπηρεσίες και ηλεκτρονικό εμπόριο, αλλά διευκολύνει και την υλοποίηση ακαδημαϊκών και επαγγελματικών εργασιών και υποχρεώσεων.

Παρ' όλα τα πλεονεκτήματά του, η πρόσβαση στο διαδίκτυο σήμερα εγκυμονεί πολλούς κινδύνους. Κακόβουλοι χρήστες, εκμεταλλευόμενοι τις ευπάθειες τόσο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και τις αδυναμίες των χρηστών προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, επιχειρώντας να αποκομίσουν κέρδος ή να επηρεάσουν κακοβούλως την λειτουργία των συστημάτων. Οι προκλήσεις αυτές δεν μπορούν να μηδενίσουν τις θετικές δυνατότητες που μπορεί το διαδίκτυο να προσφέρει, για το λόγο αυτό είναι πολύ σημαντική η ενημέρωση και η εκπαίδευση, ούτως ώστε να καλλιεργηθούν γνώσεις, στάσεις και δεξιότητες για την ασφαλή αξιοποίησή του. Η αντιμετώπιση και η αποφυγή πιθανών κινδύνων καθώς και η πρόληψη αποτελούν μερικές από τις πιο σημαντικές προκλήσεις στο διαδίκτυο.

Η ανάπτυξη μηχανισμών σάρωσης αποτέλεσε αρχικά απάντηση στους πρώτους ιούς των υπολογιστών που βασίζονταν σε αρχεία. Σήμερα, ωστόσο, πρόκειται για ένα εξαιρετικά εξελιγμένο εργαλείο ικανό να εντοπίζει ιούς Internet τύπου worm, αποστολείς μαζικής ηλεκτρονικής αλληλογραφίας, απειλές δούρειων ίππων, τοποθεσίες ψαρέματος (phising), προγράμματα εκμετάλλευσης δικτύου και άλλα. Εργαλεία όπως τα VirusTotal, AbuseIPDB, XFE, τα οποία χρησιμοποιούν μηχανισμούς σάρωσης, αποτελούν μια από τις βασικές τεχνικές αναγνώρισης και

εντοπισμού κινδύνου μέσω αναζήτησης Url ή Ip για την εύρεση κακόβουλου λογισμικού, κάνοντας την περιήγηση του χρήστη πιο ασφαλή.

1.1 Στόχος διπλωματικής εργασίας

Στόχος της παρούσας Διπλωματικής Εργασίας είναι η μελέτη και υλοποίηση μιας mobile εφαρμογής η οποία έχει ως καινοτομία την ανίχνευση και αξιολόγηση της φήμης των διευθύνσεων Url / IP χρησιμοποιώντας ταυτόχρονα API τεχνολογίες από διαφορετικές μηχανές ανίχνευσης και ανάλυσης κακόβολου λογισμικού, όπως το VirusTotal το XFE και το AbuseIPDB. Τα αποτελέσματα αυτής της συνδυαστικής αναζήτησης θα οδηγήσουν στο ασφαλές συμπέρασμα εάν μια IP ή μια διεύθυνση URL είναι κακόβουλη ή όχι. Ο χρήστης παράλληλα έχει την δυνατότητα να αποκτήσει πρόσβαση και να επεξεργαστεί τις απαντήσεις τού κάθε επιμέρους API, ενώ μέσω του ιστορικού αναζήτησης έχει τη δυνατότητα να λάβει αναλυτικές πληροφορίες σχετικά με τα δεδομένα που είχε εισάγει σε προηγούμενες αναζητήσεις καθώς επίσης τα ενδιάμεσα και τελικά αποτελέσματα των επιμέρους API.

1.2 Δομή της διπλωματικής

Στο κεφάλαιο 2 θα γίνει αναφορά σε χρήσιμες έννοιες και βασικούς ορισμούς για την κατανόηση και τον προσδιορισμό του θέματος με σαφήνεια. Στο κεφάλαιο 3 θα αναπτύξουμε τους διαφορετικές τύπους επιθέσεων στο διαδίκτυο μέσω των οποίων οι κακόβουλοι χρήστες προσπαθούν να παραβιάσουν τα σύστημα πληροφοριών ενός ατόμου ή οργανισμού. Στο κεφάλαιο 4 θα αναφερθούμε στα πλεονεκτήματα και την χρησιμότητα της API τεχνολογίας στην ασφάλειας πληροφοριακών συστημάτων, ενώ στο κεφάλαιο 5 θα μελετήσουμε και θα αναλύσουμε τους διάφορους μηχανισμούς σάρωσης για την ανίχνευση και ανάλυση κακόβουλου λογισμικού. Στο κεφάλαιο 6 γίνεται παρουσίαση της mobile εφαρμογής, που αναπτύχθηκε στα πλαίσια της εργασίας, και των δυνατοτήτων της. Τέλος, στο κεφάλαιο 7 παρουσιάζονται ενδεικτικά παραδείγματα χρήσης της εφαρμογής καθώς και τα παραγόμενα συμπεράσματα από το σύνολο της διπλωματικής εργασίας.

2. Βασικές έννοιες / Ορολογία

Η ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων καθώς αυτά μεταδίδονται μέσω των δικτύων υπολογιστών, αποτελεί έναν από τους βασικότερους παράγοντες για την ανάπτυξη ηλεκτρονικών υπηρεσιών και την επιτυχή ενσωμάτωση των δικτυακών υποδομών στην καθημερινότητα των πολιτών. Τα ζητήματα της ασφάλειας πληροφοριών στο διαδίκτυο είναι σύνθετο. Στο εισαγωγικό αυτό κεφάλαιο προκειμένου να προσδιοριστεί το θέμα της εργασίας με σαφήνεια είναι χρήσιμο να γίνει αναφορά σε μερικές βασικές έννοιες και ορισμούς.

2.1 Μοντέλο αναφοράς OSI

Το μοντέλο OSI (Open Systems Interconnection Model) είναι ένα εννοιολογικό πλαίσιο που χρησιμοποιείται για την περιγραφή των λειτουργιών ενός συστήματος δικτύωσης. Το μοντέλο OSI χαρακτηρίζει τις λειτουργίες υπολογιστών σε ένα καθολικό σύνολο κανόνων και απαιτήσεων για την υποστήριξη της διαλειτουργικότητας μεταξύ διαφορετικών προϊόντων και λογισμικού. Στο μοντέλο αναφοράς OSI, οι επικοινωνίες μεταξύ ενός υπολογιστικού συστήματος χωρίζονται σε επτά διαφορετικά επίπεδα (φυσικό επίπεδο , data, δικτύου, μεταφοράς , συνόδου, παρουσίασης , εφαρμογών).

2.2 Περιγραφή των επιπέδων OSI

Φυσικό επίπεδο

Το φυσικό επίπεδο είναι το χαμηλότερο επίπεδο του μοντέλου OSI και αφορά την ηλεκτρική ή οπτική μετάδοση ακατέργαστων μη δομημένων bits δεδομένων στο διαδίκτυο από το φυσικό στρώμα της συσκευής αποστολής στο φυσικό στρώμα της συσκευής λήψης.

Επίπεδο δεδομένων

Στο επίπεδο σύνδεσης δεδομένων, χρησιμοποιούνται απευθείας συνδεδεμένοι κόμβοι για την εκτέλεση μεταφοράς δεδομένων από κόμβο σε κόμβο όπου τα δεδομένα περιέχονται μέσα σε frames. Στο data επίπεδο σύνδεσης γίνεται διόρθωση σφαλμάτων που ενδέχεται να έχουν συμβεί στο φυσικό επίπεδο.

Επίπεδο δικτύου

Το επίπεδο δικτύου είναι υπεύθυνο για τη λήψη πλαισίων από το επίπεδο σύνδεσης δεδομένων καθώς και για την παράδοσή τους στους επιλεγμένους προορισμούς με βάση τις διευθύνσεις που περιέχονται στο πλαίσιο. Το επίπεδο δικτύου βρίσκει τον προορισμό χρησιμοποιώντας λογικές διευθύνσεις, όπως IP (πρωτόκολλο Διαδικτύου).

Επίπεδο μεταφοράς

Το επίπεδο μεταφοράς διαχειρίζεται την παράδοση και τον έλεγχο σφαλμάτων των πακέτων δεδομένων. Ρυθμίζει το μέγεθος, την αλληλουχία και τη μεταφορά δεδομένων μεταξύ συστημάτων και κεντρικών υπολογιστών. Ένα από τα πιο κοινά παραδείγματα του επιπέδου μεταφοράς είναι το TCP πρωτόκολλο.

Επίπεδο συνόδου

Το επίπεδο συνεδρίας ελέγχει τις συνομιλίες μεταξύ διαφορετικών υπολογιστών. Μια περίοδος σύνδεσης ή σύνδεση μεταξύ μηχανημάτων ρυθμίζεται, διαχειρίζεται και τερματίζεται στο επίπεδο 5. Οι υπηρεσίες επιπέδου συνεδρίας περιλαμβάνουν επίσης έλεγχο ταυτότητας και επανασυνδέσεις.

Επίπεδο παρουσίασης

Το επίπεδο παρουσίασης μορφοποιεί ή μεταφράζει δεδομένα για το επίπεδο εφαρμογής βάσει της σύνταξης ή της σημασιολογίας που δέχεται η εφαρμογή.

Επίπεδο εφαρμογών

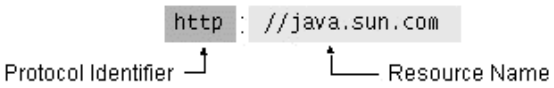
Σε αυτό το επίπεδο, τόσο ο τελικός χρήστης όσο και το επίπεδο εφαρμογής αλληλεπιδρούν απευθείας με την εφαρμογή λογισμικού. Αυτό το επίπεδο αναγνωρίζει υπηρεσίες δικτύου που παρέχονται σε εφαρμογές τελικού χρήστη.[1]

2.3 IP Address

Μια διεύθυνση **Ip (Ip address)** είναι μια μοναδική διεύθυνση με την οποία αναγνωρίζεται κάθε συσκευή που είναι συνδεδεμένη σε ένα δίκτυο που χρησιμοποιεί το πρωτόκολλο Ip. Κάθε συσκευή που συνδέεται στο διαδίκτυο λαμβάνει μια διεύθυνση Ip από τον πάροχο υπηρεσιών της (ISP). Μια διεύθυνση IPv4 γράφεται συνήθως με δεκαδικά ψηφία, μορφοποιημένα ως τέσσερα πεδία 8-bit που διαχωρίζονται με τελείες. Κάθε πεδίο 8-bit αντιπροσωπεύει ένα byte της διεύθυνσης IPv4. Η εξέλιξη της έκδοσης των IPv4 διευθύνσεων είναι η έκδοση IPv6. Μια διεύθυνση IPv6 έχει την ακόλουθη μορφή: y: y: y: y: y: y: y: y όπου y ονομάζεται τμήμα και μπορεί να είναι οποιαδήποτε δεκαεξαδική τιμή μεταξύ 0 και FFFF.[2]

2.4 URL

Το Url είναι ακρωνύμιο του Uniform Resource Locator και είναι η διεύθυνση ενός πόρου στο διαδίκτυο. Ένα χαρακτηριστικό παράδειγμα φαίνεται παρακάτω[3].



Εικόνα- 1-Url[33]

Το παράδειγμα δίνει τη διεύθυνση ενός ιστοτόπου. Το Url έχει δύο τμήματα, τα οποία χωρίζονται με "://"

- Protocol identifier: Καθορισμός πρωτοκόλλου
- Resource name: Ονομασία πόρου

Στο παράδειγμα το πρωτόκολλο επικοινωνίας είναι το Hypertext Transfer Protocol (HTTP), το οποίο αποτελεί το σύνηθες πρωτόκολλο μεταφοράς υπερκειμένου. Υπάρχουν αρκετά άλλα πρωτόκολλα, όπως τα File Transfer Protocol (FTP), File και News.[3]

2.5 Internet Control Message Protocol (ICMP)

Το Internet Control Message Protocol (ICMP) είναι ένα πρωτόκολλο επιπέδου δικτύου που χρησιμοποιείται από συσκευές δικτύου για τη διάγνωση προβλημάτων επικοινωνίας δικτύου. Το ICMP χρησιμοποιείται κυρίως για τον προσδιορισμό του κατά πόσον τα δεδομένα φθάνουν ή όχι στον προορισμό τους έγκαιρα. Συνήθως, το πρωτόκολλο ICMP χρησιμοποιείται σε συσκευές δικτύου, όπως δρομολογητές. Το ICMP είναι ζωτικής σημασίας για την αναφορά σφαλμάτων και τον έλεγχο, αλλά μπορεί επίσης να χρησιμοποιηθεί σε επιθέσεις (DDoS).[4]

3.Κυβερνοεπιθέσεις

Οι κυβερνοεπιθέσεις (cyber attacks) αποτελούν πλέον μια ισχυρή πραγματικότητα λόγω του πολλαπλασιασμού των συσκευών και της εξέλιξης των υπηρεσιών τις οποίες οι άνθρωποι χρησιμοποιούν για να επικοινωνούν μεταξύ τους διακυβεύοντας τεράστια προσωπικά και εταιρικά δεδομένα. Η κατανόηση των τύπων επίθεσης στον κυβερνοχώρο και των διαφορετικών τεχνικών που χρησιμοποιούν οι επιτιθέμενοι για την εκτέλεσή τους μπορεί να συμβάλει σημαντικά στη δημιουργία κατάλληλων πλαισίων ασφαλείας .

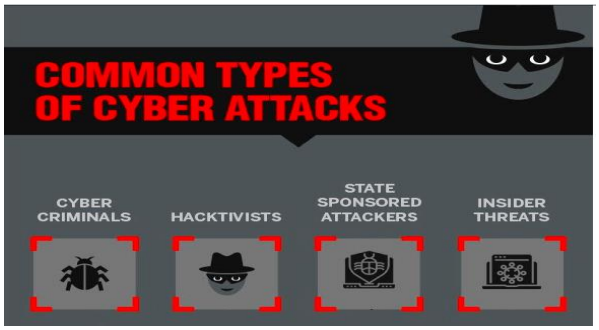
Σύμφωνα με τη Cisco, μια επίθεση στον κυβερνοχώρο είναι «μια κακόβουλη και εσκεμμένη προσπάθεια ενός ατόμου ή ενός οργανισμού να παραβιάσει το σύστημα πληροφοριών άλλου ατόμου ή οργανισμού. Οι εγκληματίες του κυβερνοχώρου πραγματοποιούν αυτές τις επιθέσεις χρησιμοποιώντας έναν ή περισσότερους υπολογιστές εκμεταλλευόμενοι τα υπάρχοντα κενά και χρησιμοποιώντας έναν ή περισσότερους φορείς επίθεσης για καταστροφή, αλλαγή, απενεργοποίηση ή απόκτηση μη εξουσιοδοτημένης πρόσβασης στους κόμβους ή τα περιουσιακά στοιχεία του

δικτύου.»**[5]**

Εικόνα- 2- Cost of cybercrime [10]

Σύμφωνα με τη μελέτη «Κόστος του εγκλήματος στον κυβερνοχώρο» της Accenture για το 2019, σημειώθηκε τεράστια αύξηση κατά 67 τοις εκατό στις παραβιάσεις ασφάλειας τα τελευταία πέντε χρόνια (Εικ.2). Η συνολική αξία του κινδύνου που προκύπτει από αυτά τα εγκλήματα στον κυβερνοχώρο υπολογίζεται να αγγίξει το ποσό των 5,2 τρισεκατομμύρια δολαρίων τα επόμενα πέντε χρόνια.

3.1 Κατηγορίες επιτιθέμενων



Εικόνα- 3 Common types of cyber-attacks [10]

Οι επιτιθέμενοι ανάλογα με την πρόθεσή και τον τελικό τους στόχο, χωρίζονται στις παρακάτω κατηγορίες. (Εικ.3)

3.1.1 Cyber-criminals

Πρόκειται για άτομα ή ομάδες ατόμων που χρησιμοποιούν την τεχνολογία για να διαπράξουν επιθέσεις σε ψηφιακά συστήματα η δίκτυα με σκοπό την κλοπή ευαίσθητων εταιρικών πληροφοριών ή προσωπικών δεδομένων καθώς και τη δημιουργία κέρδους.[5]

3.1.2 Hacktivists

Οι hacktivists είναι ομάδες εγκληματιών που οργανώνονται για να πραγματοποιήσουν επιθέσεις στον κυβερνοχώρο με στόχο την υποστήριξη πολιτικών σκοπών. Οι hacktivists στοχεύουν συνήθως σε ολόκληρες βιομηχανίες, αλλά μερικές φορές επιτίθενται σε συγκεκριμένους οργανισμούς που δεν συμφωνούν με τις πολιτικές απόψεις ή πρακτικές τους.[6]

3.1.3 State-sponsored attackers

Πραγματοποιούν κυβερνοεπιθέσεις με στόχο μια συγκεκριμένη χώρα για να αποσταθεροποιήσουν την κοινωνική, οικονομική ή στρατιωτική της διοίκηση μέσω της υποστήριξης της χώρας καταγωγής τους.

3.1.4 Insider threats

Προέρχονται από υπαλλήλους, τρίτους συνεργάτες ενός οργανισμού και είναι δύσκολο να εντοπιστούν και να αποφευχθούν λόγω του παράγοντα εμπιστοσύνης. Αυτές οι επιθέσεις θα μπορούσαν να είναι είτε κακόβουλες ή να πραγματοποιηθούν λόγω καθαρής αμέλειας.

Επιπλέον, οι κυβερνοεπιθέσεις εμπίπτουν σε δύο ομάδες με βάση το τελικό σημείο της επίθεσης:

1)Επιθέσεις στον κυβερνοχώρο μέσω διαδικτύου, εάν ο κακόβουλος στοχεύει μια ιστοσελίδα ή μια εφαρμογή ιστού.

2) Επίθεση στον κυβερνοχώρο που έχει ως στόχο το σύστημα, εάν ο σκοπός της επίθεσης προορίζεται για παραβίαση ενός συστήματος η ενός δικτύου.

3.2 Κατηγορίες Επιθέσεων

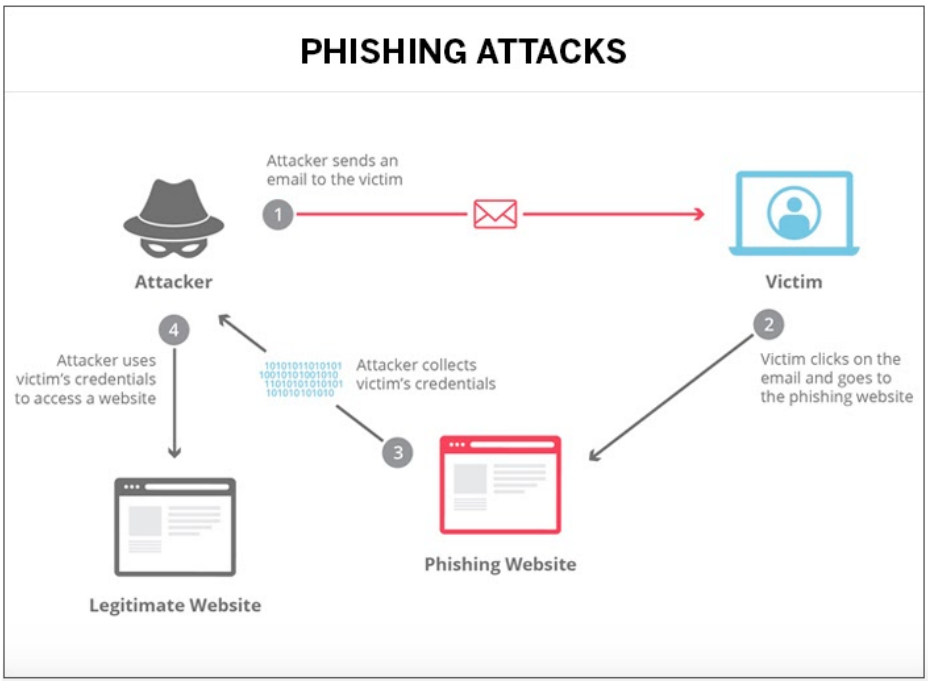
Ο ψηφιακός κόσμος είναι γεμάτος με ατελείωτες παραλλαγές κυβερνοαπειλών που προσπαθούν να διεισδύσουν στο δίκτυο και τις συσκευές των χρηστών. Δεν υπάρχει αμφιβολία ότι οι κυβερνοεπιθέσεις ήρθαν για να μείνουν και θα συνεχίσουν να υπάρχουν όσο υπάρχει το Διαδίκτυο. Ενώ οι τύποι κυβερνοεπιθέσεων συνεχίζουν να αυξάνονται, κρίνεται σημαντικό να κατανοήσουμε μερικούς από τους πιο κοινούς και διαδεδομένους τύπους επιθέσεων στο κυβερνοχώρο και παρακάτω θα να γίνει αναφορά σε κάποιες από αυτές.

3.2.1 Phishing

Το ηλεκτρονικό ψάρεμα γνωστό και ως Phishing είναι ευρέως διαδεδομένο και αυξάνεται με ταχείς ρυθμούς. Πρόκειται για μια απόπειρα κλοπής κρίσιμων personally identifiable information (προσωπικά αναγνωρίσιμων πληροφοριών), όπως διαπιστευτήρια χρήστη, οικονομικά στοιχεία, στοιχεία πιστωτικής κάρτας και οτιδήποτε έχει δυνητική αξία. Μέσω του phishing ο κακόβουλος υποδυόμενος μία αξιόπιστη οντότητα προσπαθεί να δελεάσει τον στόχο προκειμένου να του αποκαλύψει σημαντικά δεδομένα όπως ευαίσθητα ιδιωτικά στοιχεία και κωδικούς.

Τύποι επιθέσεων Phishing

Στον πυρήνα του, το ηλεκτρονικό ψάρεμα εκμεταλλεύεται τις ανθρώπινες παρορμήσεις μέσα από ένα ελκυστικό μήνυμα ή προσφορά. Οι επιτιθέμενοι συνήθως καταφεύγουν σε επιθέσεις ηλεκτρονικού ψαρέματος στοχεύοντας σε μεγάλες ομάδες και ως εκ τούτου αυξάνουν τις πιθανότητες ολοένα και περισσότερων στόχων να πέσουν θύματα της επίθεσης. Ένα τυπικό παράδειγμα μιας επίθεσης ηλεκτρονικού ψαρέματος περιλαμβάνει τον εισβολέα που συστήνεται ως ένα αξιόπιστο πρόσωπο που ανήκει σε κάποια εταιρία ή οργανισμό, στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν κάποιο συνημμένο σύνδεσμο στην επικοινωνία σε ανυποψίαστους στόχους ζητώντας άμεση βοήθεια. Ο ανυποψίαστος χρήστης ενεργοποιώντας το σύνδεσμο μεταβαίνει σε διαφορετική ιστοσελίδα από αυτή που προβλέπεται. Το άτομο, χωρίς επίγνωση της παγίδας, πέφτει σε αυτήν και καταλήγει να μοιράζεται προσωπικά στοιχεία με τον εισβολέα (Εικ.4)



Εικόνα- 4-Phishing attacks [10]

Η επίθεση phishing στηρίζεται στην έλλειψη γνώσεων των χρηστών που κάνουν χρήση του διαδικτύου, την έλλειψη προσοχής του θύματος και την οπτική εξαπάτηση. Βασικός στόχος του επιτιθεμένου είναι να πείσει το θύμα για την αυθεντικότητα και την αξιοπιστία του συνδέσμου. Αυτό το επιτυγχάνει με παραπλανητικά κείμενα, εικόνες, λογότυπα δελεάζοντας τους υποψήφιους στόχους να παραθέσουν τα προσωπικά τους δεδομένα,

Μια δεύτερη κατηγορία Phishing επίθεσης είναι το SMiShing. Το SMiShing είναι παρόμοιο με την απάτη μέσω ηλεκτρονικού ταχυδρομείου, αλλά οι κακόβουλοι παραπλανούν τους χρήστες μέσω μηνυμάτων κειμένου. Πολλοί άνθρωποι γνωρίζουν το phishing μέσω ηλεκτρονικού ταχυδρομείου, ωστόσο, λιγότεροι υποπτεύονται τα μηνύματα SMS, γεγονός που αυξάνει την πιθανότητα να πέσουν θύματα απάτης.

Αντιμετώπιση επιθέσεων Phishing

Για την καταπολέμηση των επιθέσεων ηλεκτρονικού ψαρέματος (phishing), είναι θεμιτό ο χρήστης να επαληθεύει τους αποστολείς της ηλεκτρονικής αλληλογραφίας και να κατεβάζει συνημμένα αρχεία μόνο όταν είναι απαραίτητο. Οι χρήστες-εργαζόμενοι οργανισμών και οι τρίτοι προμηθευτές θα πρέπει να εκπαιδεύονται συνεχώς

χρησιμοποιώντας μελέτες σχετικές με τη σημασία της ασφάλειας και πώς θα μπορούσαν να αποτρέψουν να πέσουν στην παγίδα ηλεκτρονικού ψαρέματος. Τα μηνύματα ηλεκτρονικού ταχυδρομείου που ζητούν οικονομική βοήθεια θα πρέπει να προκαλέσουν υποψίες στο μυαλό του χρήστη ενώ οι επιχειρήσεις πρέπει να απαγορεύουν στους υπαλλήλους τους να ανοίγουν μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από μη αξιόπιστες πηγές. Η επιλογή αξιόπιστων υπηρεσιών παροχής email με φίλτρα για spam που προσπαθούν να εξαλείψουν το email phishing δεν είναι 100% αποτελεσματικά, αλλά μπορούν να μειώσουν την απειλή.

3.2.2 Malware

Ως Malware χαρακτηρίζεται γενικά ένα ευρύ φάσμα κακόβουλων λογισμικών τα οποία εκμεταλλεύονται κενά ασφάλειας και διεισδύουν σε συστήματα-στόχους χωρίς τη συνειδητή επίγνωση και έγκριση των χρηστών. Το κακόβουλο αυτό λογισμικό παραδίδεται συνήθως με τη μορφή συνδέσμου ή αρχείου μέσω email και για να εκτελεστεί απαιτείτε από τον χρήστη να ανοίξει και να εγκαταστήσει το αρχείο. Μερικές από τις συνέπειες αποτελούν η εξαγωγή προσωπικών πληροφοριών, κωδικών πρόσβασης, κλοπή χρημάτων ακόμα και η αδυναμία πρόσβασης του χρήστη στην συσκευή.

Κατηγορίες Malware επιθέσεων

Το κακόβουλο λογισμικό διατίθεται σε διάφορες μορφές ανάλογα με τον τελικό στόχο του. Ορισμένα κακόβουλα προγράμματα σκοπεύουν να αποκτήσουν πρόσβαση σε πολλές πληροφορίες, όπως διαπιστευτήρια, στοιχεία πιστωτικών καρτών κ.λπ., ενώ άλλα είναι καθαρά προσανατολισμένα στη διακοπή υπηρεσιών. Αποτελούν οργανωμένες επιθέσεις οι οποίες προκαλούν προβλήματα σε έναν υπολογιστή, καθιστώντας το σύστημα μη λειτουργικό. Σε ορισμένες περιπτώσεις, οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν εξελιγμένο κακόβουλο λογισμικό για να μολύνουν όλα τα συστήματα στο δίκτυο. Το κακόβουλο λογισμικό έχει διάφορους τύπους και είναι χρήσιμο να γίνει αναφορά σε αυτούς καθώς και στο τρόπο με τον οποίο διανέμεται.

Ransomware

Το κακόβουλο λογισμικό ransomware, είναι ένας τύπος λογισμικού που εμποδίζει τους χρήστες να έχουν πρόσβαση στο σύστημά τους ή στα προσωπικά τους αρχεία. Προκειμένου να επανακτήσουν την πρόσβαση από τους χρήστες απαιτείται πληρωμή λύτρων. Υπάρχουν διάφοροι τρόποι με τους οποίους το ransomware μπορεί να μολύνει ένα υπολογιστή. Μία από τις πιο κοινές μεθόδους είναι μέσω malicious spam email το οποίο αποτελεί ένα ανεπιθύμητο email που χρησιμοποιείται για την παράδοση του κακόβουλου λογισμικού. Τα ηλεκτρονικά μηνύματα αυτά περιέχουν συνημμένα αρχεία όπως .doc, .pdf, .xls στα οποία έχει καταχωρηθεί το κακόβουλο λογισμικό.[7]

Virus

Ο ιός είναι ένα αυτο-πολλαπλασιαζόμενο κακόβουλο λογισμικό που προορίζεται να προκαλέσει μέγιστη ζημιά μέσω της γρήγορης εξάπλωσής του σε διάφορα μέρη του σκληρού δίσκου, συμπεριλαμβανομένων των κρίσιμων αρχείων του λειτουργικού συστήματος (OS). Εγχύεται στο υπάρχον λογισμικό και εξαπλώνεται με σκοπό να μολύνει αρχεία. Ο ιός μπορεί να εξαπλωθεί ανοίγοντας ο χρήστης ένα συνημμένο email, κάνοντας κλικ σε ένα εκτελέσιμο αρχείο, επισκέπτοντας έναν μολυσμένο ιστότοπο, ενώ μπορεί επίσης να εξαπλωθεί μέσω μολυσμένων αφαιρούμενων συσκευών αποθήκευσης, όπως μονάδες USB.

Μόλις ένας ιός μολύνει τον κεντρικό υπολογιστή, μπορεί να μολύνει το λογισμικό του συστήματος τροποποιώντας είτε διαγράφοντας αρχεία ή αλλάζοντας το partiton του σκληρού δίσκου. Μερικοί ιοί αρχίζουν να αναπαράγονται μόλις μολύνουν τον κεντρικό υπολογιστή, ενώ άλλοι ιοί θα παραμείνουν αδρανείς έως ότου ένα συγκεκριμένο trigger προκαλέσει την εκτέλεση του κακόβουλου κώδικα από τη συσκευή ή το σύστημα. Μερικοί από τους διαφορετικούς τύπους ιών αναφέρονται παρακάτω [8]

Macro-viruses

Οι ιοί μακροεντολών είναι ιοί του υπολογιστή που χρησιμοποιούν τις μακροεντολές μιας εφαρμογής για να μεταδοθούν. Αυτές οι μακροεντολές μπορούν να προκαλέσουν ζημιά στο έγγραφο ή σε άλλο λογισμικό υπολογιστή. Οι ιοί μακροεντολών είναι γραμμένοι στην ίδια γλώσσα μακροεντολής που χρησιμοποιείται για εφαρμογές λογισμικού όπως προγράμματα επεξεργασίας word, excel, pdf.

Οι παραπάνω εφαρμογές διαθέτουν ισχυρές γλώσσες μακροεντολών επιτρέποντας στους ιούς αυτούς να εκτελούνται αυτόματα όταν τα έγγραφα αυτά είναι ανοιχτά. Σε αντίθεση με τους ιούς του λειτουργικού συστήματος, οι ιοί μακροεντολών δεν προσβάλλουν το λογισμικό αλλά προσβάλλουν έγγραφα και πρότυπα. Με το άνοιγμα ενός εγγράφου ή ενός πρότυπου που περιέχει ιό μακροεντολής, επηρεάζεται το σύστημα και μεταδίδεται σε άλλα έγγραφα και πρότυπα του συστήματος. Η Microsoft στις πιο πρόσφατες εκδώσεις του word απενεργοποίησε τις μακροεντολές από προεπιλογή με αποτέλεσμα οι χάκερς να χρησιμοποιούν προγράμματα μηχανικής μάθησης για να πείσουν τους στοχευόμενους χρήστες να ενεργοποιήσουν τις μακροεντολές και να ενεργοποιήσουν τον ιό. Τέλος πρόσθεσε μια νέα δυνατότητα στο Office 2016 που επιτρέπει στους διαχειριστές ασφαλείας να ενεργοποιούν η να απενεργοποιούν επιλεκτικά τη χρήση μακροεντολών. [9]

Stealth viruses

Ένας stealth virus μπορεί να μολύνει ένα σύστημα υπολογιστή με διάφορους τρόπους. Για παράδειγμα, όταν ένας χρήστης κατεβάσει και εκτελέσει ένα κακόβουλο αρχείο μπορεί να επηρεάσει την απόδοση του υπολογιστή. Ένας stealth virus είναι σχεδιασμένος για να παραμένει ενεργά κρυμμένος από τα αντίστοιχα προγράμματα προστασίας. Αυτό το επιτυγχάνει αντιγράφοντας το μολυσμένο αρχείο σε άλλη μονάδα του δίσκου, αντικαθιστώντας το αρχικό αρχείο με ένα καθαρό**.**

Boot record virus

Οι boot record ιοί μολύνουν το bootloader και προσκολλώνται στον κύριο δίσκο εκκίνησης. Όταν το σύστημα εκκινεί, το μολυσμένο αρχείο αναζητά τον τομέα εκκίνησης (boot sector), φορτώνεται στη μνήμη και μεταδίδεται σε άλλους τομείς του σκληρού δίσκου.

Trojans

Ο ιός trojan αποτελεί ένα μηχανισμό εγκατάστασης κακόβουλου λογισμικού σε συστήματα αποκρύπτοντας έξυπνα τις προθέσεις του. Συνήθως κρύβεται σε μια γνήσια εφαρμογή (όπως παιχνίδια, λογισμικό κ.λπ.) και δημιουργεί ένα backdoor το οποίο εκμεταλλεύονται οι εισβολείς για να προκαλέσουν εκτεταμένα προβλήματα. Συνεπώς ο ιός trojan αποτελεί ένα μηχανισμό εισόδου για τους επιτιθέμενους, προκειμένου να

αποκτήσουν πρόσβαση στη συσκευή του χρήστη για περαιτέρω εκμετάλλευση. Τα Trojans δεν αυτοαντιγράφονται όπως οι ιοί.

Worm

Το worm είναι ένα ειδικό κακόβουλο λογισμικό που έχει σχεδιαστεί για να εξαπλώνεται από στοχευμένες συσκευές σε άλλους κόμβους του δικτύου, σε αντίθεση με ιούς και Trojans, που προορίζονται για συγκεκριμένες τοπικές επιθέσεις. Συνήθως διαδίδετε μέσω μηνυμάτων email και ενεργοποιείτε με το άνοιγμα ενός συνημμένου αρχείου. Είναι αρκετά ισχυρό για να διανέμεται γρήγορα (στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου σε επαφές συνδέοντας τον εαυτό του ως συνημμένο) και μπορεί να εξαπλωθεί σε άλλους υπολογιστές σε χρόνο μηδέν. Η ικανότητά του να προκαλεί ζημιά πολλαπλασιάζεται με την μη αναγνώρισή του και τη δυνατότητά του να διαδίδεται μόνο του χωρίς καμία ενεργή συμμετοχή του εισβολέα.

Cryptoloot

Πρόκειται για λογισμικό παραγωγής κρυπτονομισμάτων που χρησιμοποιεί την ισχύ της κεντρικής μονάδας επεξεργασίας (CPU) ή του επεξεργαστή γραφικών (GPU) και τους υπάρχοντες πόρους του θύματος για cryptomining – προσθέτοντας συναλλαγές στο blockchain και παράγοντας νέα νομίσματα. Ανταγωνίζεται το Coinhive, προσπαθώντας να το εκτοπίσει ζητώντας μικρότερο ποσοστό των εσόδων από τους ιστότοπους.

Emotet

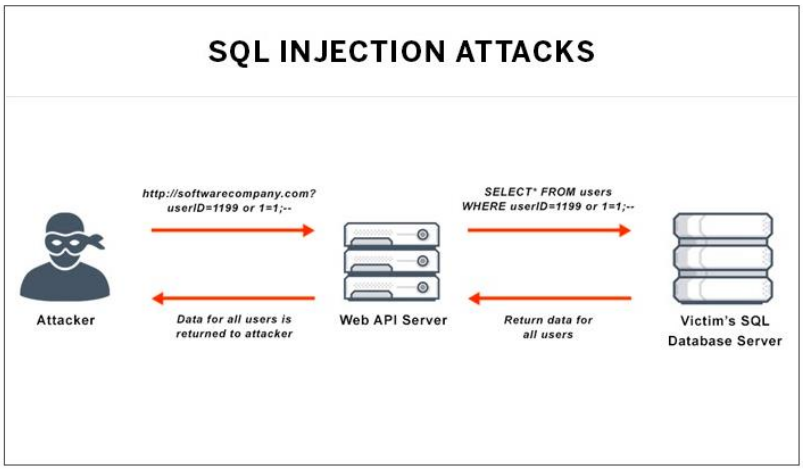
Εξελιγμένο modular Trojan που αυτοαναπαράγεται. Το Emotet κάποτε λειτουργούσε ως δούρειος ίππος υποκλοπής στοιχείων τραπεζικών λογαριασμών ενώ πρόσφατα χρησιμοποιείται για τη διανομή κακόβουλου λογισμικού ή σε εκστρατείες διάδοσης malware. Χρησιμοποιεί πολλές μεθόδους για να παραμένει στο σύστημα καθώς και τεχνικές αποφυγής ανίχνευσης. Επιπλέον, μπορεί να διαδίδεται μέσω ανεπιθύμητων email ηλεκτρονικού ψαρέματος (phishing) που περιέχουν συνημμένα ή συνδέσμους με κακόβουλο περιεχόμενο.

Αντιμετώπιση επιθέσεων malware

Οι καλύτεροι τρόποι προστασίας από επιθέσεις κακόβουλου λογισμικού είναι η εγκατάσταση λογισμικού προστασίας από ιούς, η ενημέρωση όλων των προγραμμάτων λογισμικού και η λήψη και χρήση νόμιμου λογισμικού ή εφαρμογών από αξιόπιστα καταστήματα. Η χρήση ενός δημοφιλούς λογισμικού προστασίας από ιούς βάσει συνδρομής μπορεί να βοηθήσει στον εντοπισμό τυχόν ύποπτης δραστηριότητας αρχείων με κακόβουλη πρόθεση. Αν και δεν είναι πάντα αποδοτικό, το ενημερωμένο λογισμικό προστασίας από ιούς είναι χρήσιμο να λειτουργεί ως η πρώτη γραμμή άμυνας σε περίπτωση εγκατάστασης ή επίθεσης από κακόβουλο λογισμικό. Οι προγραμματισμένοι έλεγχοι ασφαλείας των κρίσιμων για την κάθε επιχείρησή ψηφιακών στοιχείων, όπως ιστότοποι, εφαρμογές για κινητά κ.λπ., διασφαλίζουν ότι τα περιουσιακά στοιχεία είναι απαλλαγμένα από ευπάθειες ασφαλείας και εντοπίζουν τυχόν κενά για την αποφυγή εκμετάλλευσης. Η αποδοχή αυτής της αξιολόγησης κρίνεται ως υποχρεωτική δραστηριότητα καθώς προστατεύει τους πελάτες, τους υπαλλήλους και τους ενδιαφερόμενους από κάθε είδους απειλές.

3.2.3 SQL Injection

Η Structured Query Language (SQL) είναι μια γλώσσα προγραμματισμού για επικοινωνία με βάσεις δεδομένων. Οι διακομιστές χρησιμοποιούν συχνά SQL για πρόσβαση και ενημέρωση δεδομένων μεταξύ του πελάτη και της βάσης. Οι εισβολείς χρησιμοποιούν συχνά κακόβουλα SQL statements για να εξαπατήσουν τα συστήματα στην εκτέλεση ανεπιθύμητων και απροσδόκητων ενεργειών. Χρησιμοποιώντας τη μέθοδο SQL injection (SQLi), ο εισβολέας μπορεί να έχει άμεση πρόσβαση και ενημέρωση των προσωπικών στοιχείων του χρήστη από και προς τις βάσεις δεδομένων (Εικ.5). Αυτή η επίθεση βρίσκεται στην λίστα με τις 10 πιο επικίνδυνες επιθέσεις ασφαλείας της εφαρμογής OWASP(Open Web Application Security Project)



Εικόνα- 5- Sql injection attacks [10]

Μερικές από τις επιπτώσεις μιας επιτυχημένης επίθεσης SQLi περιλαμβάνουν:

- Παράκαμψη ελέγχου ταυτότητας χρήστη χωρίς όνομα χρήστη / κωδικό πρόσβασης
- Τροποποίηση / προσθήκη / διαγραφή δεδομένων από βάσεις δεδομένων και παραβίαση της ακεραιότητας των δεδομένων
- Ανάκτηση βαθμολογιών δεδομένων πελατών
- Απόκτηση πρόσβασης διαχειριστή / root μιας εφαρμογής
- Εκτέλεση OS shell και απομακρυσμένων εντολών

Σε αντίθεση με το κακόβουλο λογισμικό και το ηλεκτρονικό ψάρεμα (phishing), το SQLi απαιτεί βαθιά κατανόηση του τρόπου λειτουργίας των εφαρμογών ιστού και του μοντέλου πελάτη-διακομιστή αρχιτεκτονικής βάσης δεδομένων. Ο εισβολέας παρατηρεί συχνά προσεκτικά τη συμπεριφορά του συστήματος για μήνες πριν ξεκινήσει την επίθεση χρησιμοποιώντας έναν κατάλληλο φορέα. Το SQLi εκμεταλλεύεται ευπάθειες που προκύπτουν από τη χρήση δυναμικής SQL σε εφαρμογές ιστού, η οποία εμφανίζεται συνήθως σε εφαρμογές PHP και ASP.[10]

Κατηγορίες επιθέσεων SQLi

Παραδοσιακά, μπορούμε να ταξινομήσουμε τους τύπους έγχυσης SQL σύμφωνα με τη τον τύπο δεδομένων εισόδου, την απόκριση διακομιστή το κανάλι εξαγωγής δεδομένων και χωρίζονται σε διάφορες κατηγορίες όπως η Blind SQL Injection και η Second-Order SQL Injection.

Blind SQL Injection

Πρόκειται για μια προηγμένη τεχνική επίθεσης SQLi και χρησιμοποιείται όταν η ιστοσελίδα δεν εμφανίζει απευθείας τα δεδομένα χρήστη. Χρησιμοποιώντας το Blind SQLi, ο εισβολέας αναγνωρίζει, αποκτά ευαίσθητες πληροφορίες και τροποποιεί το περιεχόμενο της βάσης δεδομένων. Συνήθως οι επιθέσεις αυτές εκτελούνται χρησιμοποιώντας τη λειτουργία SQL sleep δίνοντας εντολή στη βάση δεδομένων να μείνει εκτός λειτουργίας για μια καθορισμένη διάρκεια καθυστερώντας τις απαντήσεις κατά τη διάρκεια αυτής της χρονικής περιόδου.

Second-Order SQL Injection

Αυτοί οι τύποι επιθέσεων χρησιμοποιούν δεδομένα που έχουν υποβληθεί από τον χρήστη και αποθηκεύονται στη βάση δεδομένων, ο εισβολέας τα ανακτά και τα χρησιμοποιεί σε μια κακόβουλη δήλωση SQL. Χρησιμοποιούν δευτερεύουσα συμπεριφορά συστήματος (όπως εργασία που ενεργοποιείται από τον διαχειριστή) για να ενεργοποιήσουν και να επιτρέψουν στον εισβολέα να ελέγξει τη βάση δεδομένων.

Προστασία από SQLi Attacks

Η πρόληψη επιθέσεων SQLi απαιτεί ισχυρές πρακτικές κωδικοποίησης. Οι προγραμματιστές θα πρέπει να αποφεύγουν τη χρήση δυναμικής SQL στα ερωτήματά τους όσο το δυνατόν περισσότερο. Οι διαχειριστές θα πρέπει να αποκτήσουν πλήρη γνώση όλων των SQL Servers του δικτύου ευθύνης τους ενώ θα πρέπει να απαγορευτεί η πρόσβαση σε συγκεκριμένα ports των servers από χρήστες αγνώστου προελεύσεως. Παρ’ όλο που μία τέτοια στρατηγική δε θεωρείται ότι παρέχει υψηλό ποσοστό ασφάλειας, ειδικά σε SQL injection επιθέσεις, αποτελεί ένα πρώτο βήμα για τη διαμόρφωση ενός γενικότερου πλέγματος ασφάλειας του πληροφορικού δικτύου μιας εταιρείας ή ενός οργανισμού. Τέλος, η άμεση εγκατάσταση των updates που αναρτώνται από τις εταιρείες σχεδίασης των λογισμικών που χρησιμοποιούνται, η

υιοθέτηση ισχυρών admin-passwords και συχνή εναλλαγή τους κρίνονται ως επιβεβλημένες ενέργειες. Η ενημέρωση και η επιδιόρθωση ζητημάτων βάσεων δεδομένων σε τακτά χρονικά διαστήματα διατηρούν τη βάση δεδομένων ασφαλή. [11]

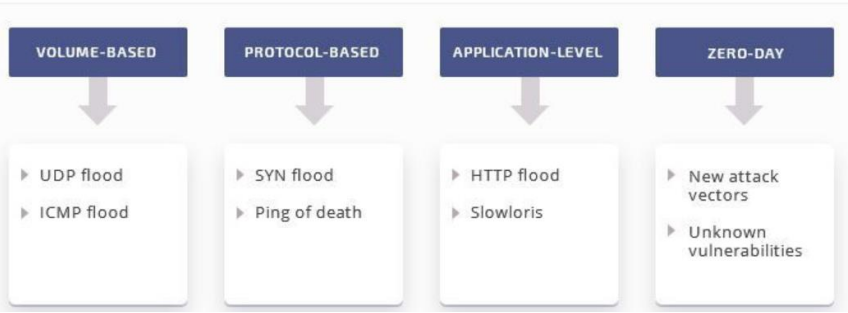
3.2.4 Denial of Service or Distributed Denial of Service Attacks - (DoS or DDoS)

Με την Ddos επίθεση οι κακόβουλοι χρήστες επιδιώκουν να καταστεί μη διαθέσιμη η παροχή μιας υπηρεσίας, κατακλύζοντάς την με κίνηση από πολλές πηγές χωρίς ο επιτιθέμενος να χρειαστεί να εκμεταλλευτεί αδυναμίες εφαρμογών η πρωτοκόλλων για να διεισδύσει σε ένα δίκτυο ή κάποιο υπολογιστικό σύστημα. Συνεπώς, βασικός σκοπός των επιθέσεων αυτών είναι να θέσουν εκτός λειτουργίας τον εξυπηρετητή στόχο.

Αν και η επίθεση DoS / DdoS δεν παρέχει κανένα άμεσο οικονομικό όφελος στον εισβολέα, η απλή ικανοποίηση της άρνησης νόμιμων αιτημάτων των χρηστών αρκεί για ορισμένους επιτιθέμενους προκειμένου να πραγματοποιήσουν αυτές τις επιθέσεις.

Κατηγορίες επιθέσεων DoS/DdoS

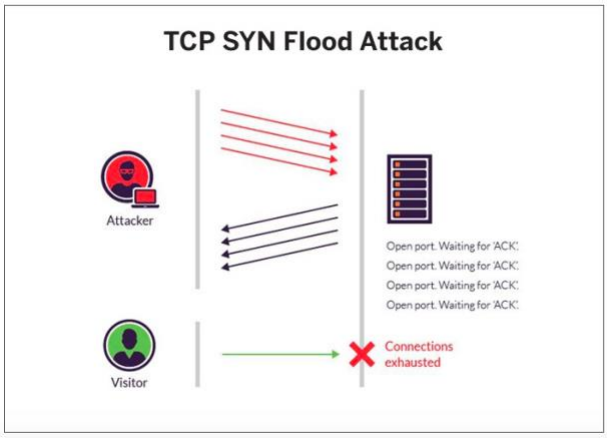
Οι κατηγορίες επιθέσεων denial of service μπορούν να κατηγοριοποιηθούν σε τέσσερις κατηγορίες ανάλογα με το επίπεδο του πρωτοκόλλου στο οποίο πραγματοποιείται και η επίθεση όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα- 6- Ddos categories [34]

Ακολουθούν ορισμένοι κοινοί τύποι επιθέσεων DdoS:

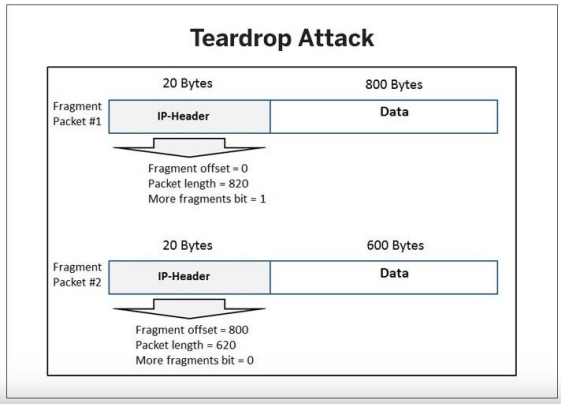
TCP SYN Flood Attack



Εικόνα- 7 -Tcp syn flood attack [10]

Το αποτέλεσμα της επίθεσης αυτής συνεπάγεται το flood του συστήματος με πολλαπλές αιτήσεις σύνδεσης και εκμετάλλευση του χώρου αποθήκευσης κατά τη διάρκεια χειραψίας προετοιμασίας περιόδου σύνδεσης πρωτόκολλου ελέγχου μετάδοσης (TCP) (Εικ.7). Το σύστημα του εισβολέα δεν ανταποκρίνεται σκόπιμα στο αίτημα από το σύστημα προορισμού και πλημμυρίζει το σύστημα με αιτήματα. Αυτό κάνει το σύστημα προορισμού να λήξει και να μην είναι διαθέσιμο για νόμιμα αιτήματα από άλλους χρήστες. [10]

Teardrop Attack



Εικόνα- 8- Teardrop attack [10]

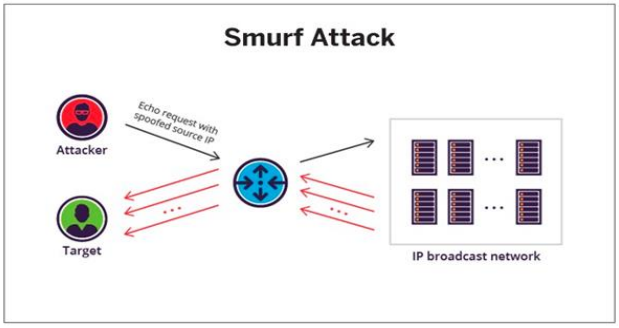
Η επίθεση αυτή περιλαμβάνει την αποστολή κατακερματισμένων πακέτων πληροφοριών σε ένα σύστημα προορισμού. Η επίθεση στοχεύει σε σφάλματα επανασυναρμολόγησης κατακερματισμού TCP / IP (βρίσκονται σε παλαιότερες εκδόσεις λειτουργικού συστήματος) και προκαλεί αλληλοεπικάλυψη κατακερματισμένων πακέτων στο σύστημα προορισμού (Εικ.8). Αν και το σύστημα προσπαθεί να ανακατασκευάσει τα κατακερματισμένα πακέτα, αποτυγχάνει και καταρρέει.[10]

User Datagram Protocol (UDP) Flood

Η UDP flood είναι ένας τύπος επίθεσης άρνησης υπηρεσίας (DoS) στην οποία ο εισβολέας κατακλύζει τυχαίες θύρες στον στοχευόμενο κεντρικό υπολογιστή με πακέτα Ip που περιέχουν UDP datagrams. Ο κεντρικός υπολογιστής ο οποίος ελέγχει για εφαρμογές που σχετίζονται με αυτά τα διαγράμματα μην ακούοντας κάποια υπηρεσία στην συγκεκριμένη πόρτα θα απαντήσει με ένα πακέτο ICMP Destination Unreachable. Καθώς όλο και περισσότερα πακέτα UDP λαμβάνονται και απαντώνται, το σύστημα υπερφορτώνετε και παύει να ανταποκρίνεται.[12]

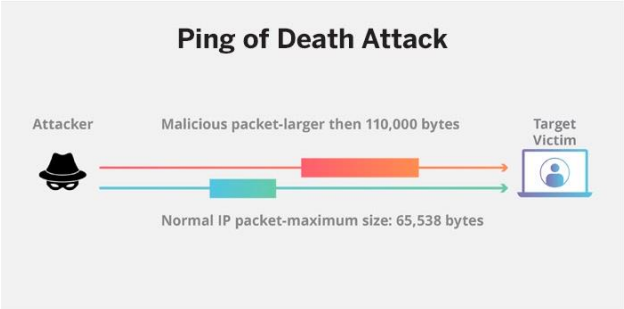
Smurf Attack

Η επίθεση Smurf είναι μια μορφή επίθεσης (DdoS) που καθιστά τα δίκτυα υπολογιστών μη λειτουργικά. Το πρόγραμμα Smurf, αξιοποιώντας τις ευπάθειες του Πρωτοκόλλου Διαδικτύου (Ip) και του Πρωτοκόλλου Μήνυμα Ελέγχου Διαδικτύου (ICMP) επιτυγχάνει να σταλεί μεγάλος αριθμός πακέτων πρωτοκόλλου (ICMP) με την Spoof Ip του θύματος σε ένα δίκτυο υπολογιστή χρησιμοποιώντας μια διεύθυνση εκπομπής Ip (Εικ.9). Οι περισσότερες από τις συσκευές σε ένα δίκτυο θα απαντήσουν από προεπιλογή σε αυτό αποστέλλοντας μια απάντηση στη διεύθυνση Ip της πηγής. Εάν ο αριθμός των μηχανών στο δίκτυο που λαμβάνουν και ανταποκρίνονται σε αυτά τα πακέτα είναι πολύ μεγάλος, ο υπολογιστής του θύματος θα πλημμυρίσει από traffic με αποτέλεσμα ο υπολογιστής να μην ανταποκρίνεται και να είναι αδύνατο να εργαστεί.[13]



Εικόνα- 9- Smurf attack [10]

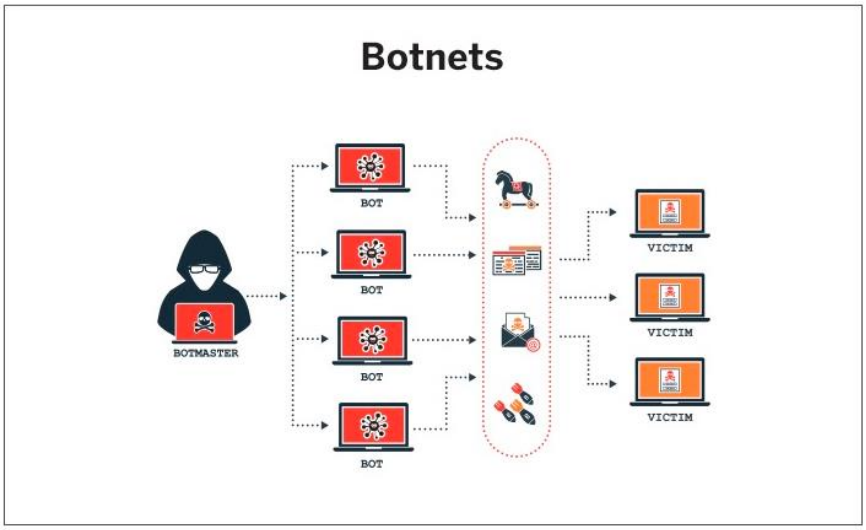
Επίθεση Ping of Death



Εικόνα- 10-Ping of death attacks [10]

Το Ping of Death (γνωστό ως PoD) είναι ένας τύπος επίθεσης άρνησης υπηρεσίας (DoS) στην οποία ένας εισβολέας προσπαθεί να συντρίψει, να αποσταθεροποιήσει ή να παγώσει τον στοχευμένο υπολογιστή ή υπηρεσία στέλνοντας παραμορφωμένα ή υπερμεγέθη πακέτα χρησιμοποιώντας μια απλή εντολή ping (Εικ.10). Κατά συνέπεια, η επίθεση Ping Of Death περιλαμβάνει την συνεχή αποστολή μεγάλων πακέτων ping σε κάποιον υπολογιστή μέχρι οι υπηρεσίες του τελευταίου να τεθούν εκτός λειτουργίας.[14]

Botnets



Εικόνα- 11- Botnet [10]

Το botnet είναι μια συλλογή συσκευών συνδεδεμένων στο Διαδίκτυο, μολυσμένων από κακόβουλο λογισμικό, που επιτρέπει στους χάκερς να τις ελέγχουν. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν botnets για να υποκινούν τις ομώνυμες επιθέσεις, οι οποίες περιλαμβάνουν κακόβουλες δραστηριότητες όπως διαρροές διαπιστευτηρίων, μη εξουσιοδοτημένη πρόσβαση, κλοπή δεδομένων και επιθέσεις DdoS.[10][16]

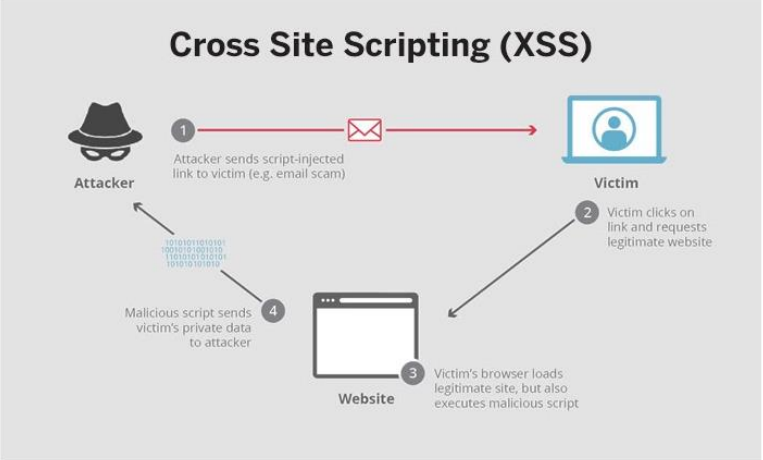
Αντιμετώπιση επιθέσεων DoS/DdoS

Η καταπολέμηση των DdoS επιθέσεων είναι αρκετά δύσκολη, καθώς είναι σχεδόν αδύνατο να εντοπίσουμε τον εισβολέα και να γνωρίζουμε την πηγή της επίθεσης. Δεδομένου ότι είναι καλύτερο να αποτραπεί μια επίθεση DoS / DdoS πριν την εμφάνιση της η χρήση εργαλείων ασφάλειας και περιμέτρου δικτύου για την παρακολούθηση του traffic συνήθως βοηθά στην αντιμετώπιση τους.

Το monitoring για ύποπτες δραστηριότητες στο δίκτυο θα μπορούσε να αποτελεί βασική λύση. Για παράδειγμα, η ασυνήθιστη κίνηση στο διαδίκτυο θα πρέπει να προκαλεί συναγερμό και κατά συνέπεια να μπλοκάρεται. Οι διαχειριστές ιστού θα πρέπει να χρησιμοποιούν μεθόδους φιλτραρίσματος αποκλείοντας πλαστές διευθύνσεις Ip.

Ορθή πρακτική αποτελεί και η απενεργοποίηση των θυρών που δε χρησιμοποιούνται, ώστε οι εγκληματίες του κυβερνοχώρου να μην εκμεταλλεύονται μια πιθανή ευπάθεια. Επίσης, η απενεργοποίηση εκπομπών κατευθυνόμενων Ip σε επίπεδο δρομολογητών μπορεί να αποβεί χρήσιμη. Η διαμόρφωση των τειχών προστασίας για το χειρισμό πακέτων SYN και της παρακολούθησης κατακερματισμένων payload για το μέγιστο μέγεθός τους παίζουν σημαντικό ρόλο στην αποφυγή επιθέσεων DdoS. Η χρήση διευθύνσεων διακομιστή μεσολάβησης (proxy addresses) μπορεί επίσης να είναι χρήσιμη για την προστασία από επιθέσεις DdoS Cross-Site.

3.2.5 Scripting (XSS)



Εικόνα- 12 – Cross site scripting [10]

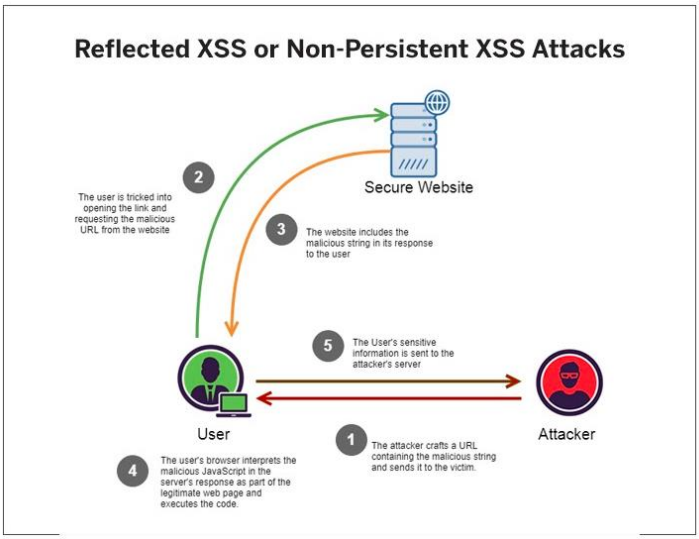
Οι λειτουργίες XSS αποτελούν εξέχουσα απειλή στους κινδύνους ασφαλείας των 10 κορυφαίων εφαρμογών OWASP. Είναι μια ομάδα επιθέσεων όπου ο εισβολέας εισάγει κώδικα ή κακόβουλα σενάρια απευθείας σε έναν καλοήθη ιστότοπο χωρίς να επιτίθεται σε αυτόν. Ο εισβολέας γράφει το σενάριο σε JavaScript, Flash, Ajax κ.λπ.

Κάθε φορά που ένας χρήστης επισκέπτεται έναν παραβιασμένο ιστότοπο, το πρόγραμμα περιήγησής του εκτελεί το σενάριο. Δεδομένου ότι το πρόγραμμα περιήγησης ιστού δεν αναγνωρίζει το κακόβουλο σενάριο, καθώς προέρχεται από μια αξιόπιστη πηγή, αυτό εκτελείται με επιτυχία και καταγράφει cookies, διακριτικά περιόδου λειτουργίας και άλλες ευαίσθητες πληροφορίες που διατηρούνται από το πρόγραμμα περιήγησης. Αυτό όχι μόνο βλάπτει τη φήμη του ιστότοπου, αλλά επίσης παραβιάζει τυχόν πληροφορίες που ο χρήστης ανταλλάσσει μαζί του, όπως

διαπιστευτήρια χρήστη, πληροφορίες πιστωτικής κάρτας, cookie κ.λπ. Στις περιπτώσεις των XSS επιθέσεων, τόσο ο χρήστης όσο και ο διαχειριστής του συστήματος δεν έχουν καμία ένδειξη του malicious κώδικα που έχει τεθεί σε εφαρμογή γεγονός που θα μπορούσε να προκαλέσει τεράστιες επιπτώσεις εάν δεν αντιμετωπιστεί άμεσα.[10]

Κατηγορίες επιθέσεων XSS

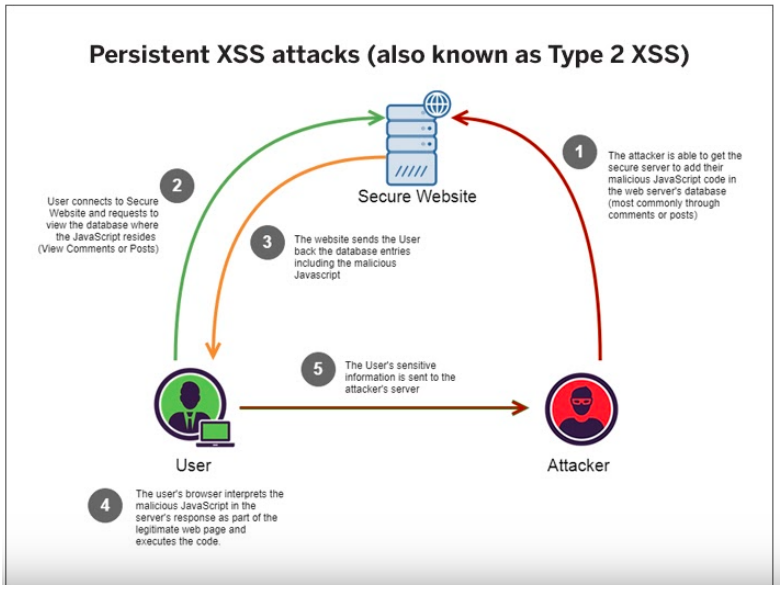
Reflected XSS or Non-Persistent XSS Attacks



Εικόνα- 13- Reflected XSS or Non Persistent XSS attack [10]

Αυτοί οι τύποι επιθέσεων συμβαίνουν όταν η εφαρμογή λαμβάνει δεδομένα σε αίτημα HTTP αλλά παραλαμβάνει την απόκριση με μη ασφαλή τρόπο. Ο εισβολέας μεταβιβάζει το κακόβουλο σενάριο ως ερώτημα στη διεύθυνση Url και το δημοσιεύει ως σύνδεσμο ή το στέλνει σε ένα email (phishing mail) στον χρήστη (Εικ.13). Όταν ο χρήστης κάνει κλικ στον σύνδεσμο, το σενάριο εκτελείται. Επειδή το ερώτημα έχει μη εισαγόμενες τιμές εισόδου, το κακόβουλο σενάριο εισάγετε στην ιστοσελίδα που φορτώνει το πρόγραμμα περιήγησης του συστήματος στόχου και εκτελείται από το πρόγραμμα περιήγησης και ο επιτιθέμενος λαμβάνει ιδιωτικά δεδομένα. Σε περίπτωση περίπλοκων επιθέσεων, ο εισβολέας μπορεί να εκτελέσει οποιαδήποτε ενέργεια στην εφαρμογή ως χρήστης και ακόμη και να ξεκινήσει αλληλεπιδράσεις με άλλους χρήστες. [10]

Persistent XSS attacks



Εικόνα- 14-Persistent XSS attack (also known as Type 2 XSS [10]

Οι επιθέσεις αυτές συμβαίνουν όταν ο εισβολέας αποθηκεύει την είσοδο χρήστη στον ίδιο τον ευάλωτο διακομιστή χωρίς να εκτελεί σωστή επικύρωση. Άλλοι χρήστες που επισκέπτονται τον παραβιασμένο ιστότοπο λαμβάνουν τις αποθηκευμένες εισόδους και εκτελούν το κακόβουλο σενάριο στο τοπικό τους πρόγραμμα περιήγησης, χωρίς να εκτελούν καμία ενέργεια (Εικ.14). Αν και είναι λιγότερο διαδεδομένες, οι συνέπειες τους είναι καταστροφικές.[10]

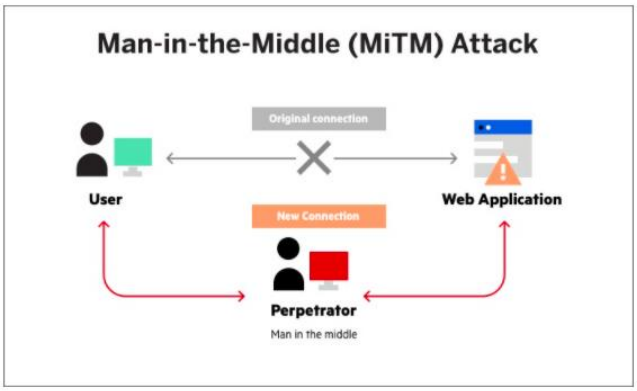
Αντιμετώπιση επιθέσεων XSS

Η πρόληψη των επιθέσεων XSS που αναφέρονται παραπάνω απαιτεί επαρκή μέτρα ασφαλείας τόσο από την πλευρά του πελάτη όσο και από του διακομιστή. Κρίνεται σημαντικό οι χρήστες να χρησιμοποιούν ασφαλείς πρακτικές κωδικοποίησης, όπως ενσωματωμένες λειτουργίες καθαρισμού και επικύρωσης.

Είναι ζωτικής σημασίας να πραγματοποιείται χειροκίνητη αλλαγή στη βάση κώδικα και απαιτείται η λήψη βοηθητικών εργαλείων δοκιμών ασφαλείας για την εύρεση πιθανών αποθηκευμένων XSS. Επιπρόσθετα, απαιτείται η διόρθωση των αναγνωρισμένων τρωτών σημείων προτού ο ενεργοποιηθεί ένας ιστότοπος. Η τακτική χρήση ενός εργαλείου σάρωσης ευπάθειας εφαρμογών ιστού θα μπορούσε να βοηθήσει

τους προγραμματιστές να εντοπίσουν τρωτά σημεία στην εφαρμογή και να τα αποκαταστήσουν αποτελεσματικά.

3.2.6 Man-in-the-Middle (MiTM) επίθεση

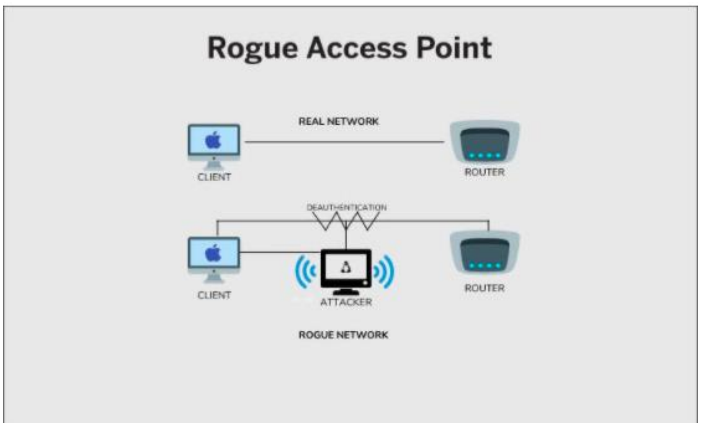


Εικόνα- 15– Man in the Middle attack [10]

Οι επιθέσεις MiTM συμβαίνουν όταν η κακόβουλη οντότητα ακούει την επικοινωνία μεταξύ client και του server. Κάθε αλληλεπίδραση μεταξύ του client και του server λαμβάνει ένα αναγνωριστικό περιόδου σύνδεσης, το οποίο είναι ιδιωτικό για αυτούς (Εικ.15). Όμως, σε περίπτωση επίθεσης MiTM, ο επιτιθέμενος εισβάλλει στη συνεδρία (μέσω της επίθεσης XSS, για παράδειγμα) καταγράφοντας το αναγνωριστικό περιόδου (session id) και προσποιούμενος την πραγματική πηγή συνεχίζει τη συνεδρία με τον διακομιστή για λογαριασμό του χρήστη. Ο εισβολέας αποκτά πρόσβαση σε μη εξουσιοδοτημένα σύνολα πληροφοριών στο διακομιστή και μπορεί να προκαλέσει καταστροφή. Αυτή η επίθεση έρχεται σε πολλές μορφές, όπως η πλαστογράφηση Ip και DNS, η επίθεση επανάληψης (replay attack) και η πειρατεία συνεδρίας (session hijacking).[10]

Κατηγορίες MiTM επιθέσεων

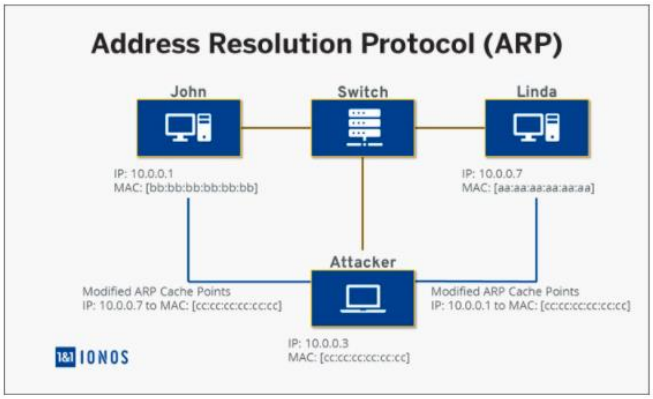
Rogue Access Point



Εικόνα- 16– Rogue Access attack [10]

Το rogue access point ορίζεται ως οποιοδήποτε ασύρματο σημείο πρόσβασης που δεν είναι μέρος του δικτύου. Οι κακόβουλοι χρησιμοποιώντας τέτοια ανοιχτά σημεία ασύρματης πρόσβασης επιχειρούν να αποκτήσουν πρόσβαση σε κοντινές συσκευές (Εικ.16). Συνήθως δεν υπάρχουν μηχανισμοί κρυπτογράφησης ή ελέγχου ταυτότητας, έτσι ώστε να μπορούν να συνδεθούν οι μέγιστες συσκευές που βρίσκονται σε κοντινή απόσταση. Ο κακόβουλος επομένως θέτει σε κίνδυνο τα δεδομένα δικτύου.[10]

Address Resolution Protocol (ARP) Spoofing



Εικόνα- 17 – Address Resolution Protocol [10]

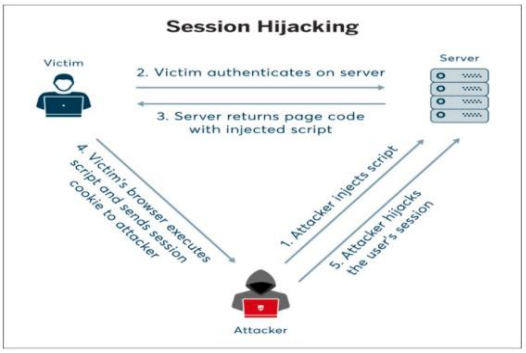
Το ARP (address resolution protocol) είναι μια διαδικασία για το mapping μιας δυναμικής διεύθυνσης πρωτοκόλλου Διαδικτύου (διεύθυνση IP) σε μια μόνιμη φυσική

διεύθυνση μηχανήματος σε τοπικό δίκτυο (LAN). Η διεύθυνση του φυσικού μηχανήματος είναι επίσης γνωστή ως έλεγχος πρόσβασης πολυμέσων ή διεύθυνση MAC. Χρησιμοποιώντας ARP spoofing, ο εισβολέας στέλνει ψεύτικα/πλαστογραφημένα μηνύματα ARP. Αυτό αναγκάζει τη διεύθυνση MAC να χαρτογραφηθεί με τη διεύθυνση ενός νόμιμου υπολογιστή στο δίκτυο (Εικ.17). Αυτό έχει ως αποτέλεσμα ο εισβολέας να λάβει πληροφορίες που προορίζονται για το αρχικό σύστημα, να παρακολουθεί και να τροποποιεί τα δεδομένα κατά τη μεταφορά.[17][10]

Multicast DNS (mDNS) επίθεση

Σε αυτό τον τύπο επίθεσης , ένα ερώτημα DNS αποστέλλεται σε όλες τις συσκευές του δικτύου στον ίδιο broadcast domain. Ο επιτιθέμενος πραγματοποιεί επίθεση mDNS spoofing στο LAN, όπως και το ARP spoofing, με τους χρήστες να μην χρειάζεται απαραίτητα να θυμούνται τις διευθύνσεις με τις οποίες συνδέονται. Ο εισβολέας χρησιμοποιεί αυτό το πρωτόκολλο κάνοντας request με ψεύτικα δεδομένα και συνδέεται στο σύστημα ως αξιόπιστο δίκτυο. Το σύστημα του θύματος θα αποδεχθεί τη συσκευή του εισβολέα ως αξιόπιστο δίκτυο, το οποίο μπορεί στη συνέχεια να ελέγξει τη συσκευή.

Session Hijacking



Εικόνα- 18– Session Hijacking [10]

Η παραβίαση συνεδρίας (session hijacking) αποτελεί ένα διάνυσμα επίθεσης MiTM. Μέσω του XSS, ο εισβολέας αποκτά πρόσβαση στο διακριτικό περιόδου σύνδεσης του χρήστη (user session token) και πλαστοπροσωπεί τις δραστηριότητες του. Αφού ο εισβολέας αποκτήσει πρόσβαση στο session token, αποκτά πλήρη πρόσβαση στα δικαιώματα του χρήστη στην εφαρμογή.

Αντιμετώπιση MiTM επίθεσης

Η πρόληψη αντιμετώπισης των επιθέσεων MiTM πριν ακόμα εμφανιστούν αποτελούν ένα ενδεδειγμένο τρόπο για την αποφυγή τους. Η εφαρμογή ισχυρής κρυπτογράφησης προστατευμένης πρόσβασης Wi-Fi σε σημεία πρόσβασης είναι ένας σίγουρος τρόπος για την αποτροπή επιθέσεων MiTM. Τα εικονικά ιδιωτικά δίκτυα (VPN) αποτελούν τον ιδανικό τρόπο ανταλλαγής ευαίσθητων πληροφοριών σε ένα δίκτυο μέσω κρυπτογραφημένης επικοινωνίας. Αυτό καθιστά δύσκολο για τους εισβολείς να αποκρυπτογραφήσουν την επικοινωνία δικτύου και να καλύψουν την πραγματική τοποθεσία των χρηστών. Το ασφαλές επίπεδο μιας δικτυακής σύνδεσης στο HTTPS βοηθά στην αποφυγή παραβίασης των εισβολέων με την επικοινωνία που λαμβάνει χώρα μεταξύ του πελάτη και του διακομιστή καθώς τα δεδομένα τα οποία ανταλλάσσονται είναι κρυπτογραφημένα.

Πρωτόκολλα ελέγχου ταυτότητας που βασίζονται σε ζεύγη δημόσιων κλειδιών, όπως το RSA, μπορούν επίσης να βοηθήσουν στην εξασφάλιση της επικοινωνίας μεταξύ δύο κεντρικών υπολογιστών με καθορισμένες διαδικασίες κρυπτογράφησης δημόσιου-ιδιωτικού τομέα και αποκρυπτογράφησης.

3.2.7 Zero-Day επίθεση

Η zero day είναι μια ευπάθεια λογισμικού υπολογιστή που είναι άγνωστη σε εκείνους που θα πρέπει να την αντιμετωπίσουν Με τις zero day επιθέσεις, ο επιτιθέμενος προσπαθεί να εκμεταλλευτεί συγκεκριμένα κενά ασφαλείας σε εφαρμογές ηλεκτρονικών υπολογιστών, τα οποία προέρχονται από λάθη των σχεδιαστών που δημιούργησαν τις εφαρμογές. Πολλές είναι επίσης οι φορές που οι σχεδιαστές δεν γνωρίζουν καν αυτά τα κενά ασφαλείας στις εφαρμογές τους, μέχρι και την πραγματοποίηση των zero day επιθέσεων. Σε πολλές περιπτώσεις, η ευπάθεια μπορεί να μην ανιχνευθεί για μήνες, με τους προγραμματιστές να γνωρίζουν το σφάλμα μόνο μετά την επίθεση, και τα συμπτώματα που προκύπτουν εμφανίζονται ως απώλεια πληροφοριών πελατών ή κλοπή διαπιστευτηρίων. Στη συνέχεια, οι προγραμματιστές αναπτύσσουν μια ενημέρωση κώδικα για την ευπάθεια και αποτρέπουν περαιτέρω ζημιές.[18]

Κατηγορίες zero day επιθέσεων

Ο εισβολέας περνά από εκατομμύρια γραμμές κώδικα, διερευνώντας εφαρμογές για τις ευπάθειές τους χρησιμοποιώντας reverse engineering εργαλεία και τεχνικές για να αποκαλύψει σφάλματα ή μη ασφαλή κώδικα. Τυπικοί στόχοι για εκμετάλλευση zero day επιθέσεων περιλαμβάνουν επιθέσεις σε κυβερνητικές υπηρεσίες, μεγάλες επιχειρήσεις, άτομα με πρόσβαση σε πολύτιμα επιχειρηματικά δεδομένα και μεγάλο αριθμό οικιακών χρηστών που χρησιμοποιούν ευάλωτο λειτουργικό σύστημα. Οι επιτιθέμενοι χρησιμοποιούν τις ευπάθειες για να θέσουν σε κίνδυνο υπολογιστές και να δημιουργήσουν τεράστια botnets. Σε ορισμένες περιπτώσεις, οι κυβερνήσεις χρησιμοποιούν zero day exploits για να επιτεθούν σε άτομα, οργανισμούς ή χώρες που απειλούν τη φυσική τους ασφάλεια.[19]

Αντιμετώπιση επιθέσεων Zero-Day

Είναι σημαντικό να εντοπιστούν ευπάθειες zero day προτού χρησιμοποιηθούν ακατάλληλα από εισβολείς. Οι έλεγχοι για σφάλματα και κενά ασφαλείας στα συστήματα μπορούν να βοηθήσουν στον εντοπισμό ευπαθειών zero day. Κάθε εφαρμογή μπορεί να γίνει πιο ασφαλής και χωρίς σφάλματα με την προσομοίωση πραγματικών σεναρίων δοκιμών επίθεσης. Η αυστηρή δοκιμή για την ανίχνευση σφαλμάτων / ευάλωτου κώδικα είναι απαραίτητη για την αποτροπή zero day επιθέσεων. Με την υιοθέτηση ευέλικτης ανάπτυξης λογισμικού, οι έλεγχοι έχουν γίνει πιο σύντομοι και πιο αποτελεσματικοί. Οι προγραμματισμένες δοκιμές μπορούν να βοηθήσουν τις ομάδες ανάπτυξης να διασφαλίσουν την ποιότητα των προϊόντων τους εντός των συμφωνημένων προθεσμιών των πελατών. Η καθιέρωση της διαχείρισης ενημέρωσης κώδικα με συγκεκριμένα patches μπορεί να μειώσει τον κίνδυνο zero day.

3.2.8 Οι πιο διαδεδομένες απειλές κακόβουλου λογισμικού σε κινητές συσκευές

Η αυξημένη χρήση κινητών συσκευών οδήγησε σε αύξηση των απειλών σχετικά με την ασφάλεια τους. Πλέον, οι χρήστες θα πρέπει να είναι πιο επιμελείς από ποτέ για να προστατεύσουν τα προσωπικά τους δεδομένα. Μερικές από τις πιο γνωστές επιθέσεις σε συσκευές κινητής τηλεφωνίας παρατίθενται παρακάτω.

Hiddad

Το Hiddad είναι ένα κακόβουλο λογισμικό στο λειτουργικό σύστημα του Android το οποίο ανασκευάζει νόμιμες εφαρμογές και στη συνεχεία τις καθιστά διαθέσιμες σε third-party κατάστημα. Η βασική του λειτουργία είναι η εμφάνιση διαφημίσεων στο χρήστη ενώ παράλληλα είναι ικανό να αποκτά πρόσβαση σε σημαντικά στοιχεία ασφάλειας που ενσωματώνονται στο λειτουργικό σύστημα, επιτρέποντας σε κάποιον εισβολέα να αποκτά και αυτός πρόσβαση σε ευαίσθητα δεδομένα του χρήστη.

Lotoor

Το lotoor αποτελεί ένα εργαλείο κυβερνοπειρατείας (hacking) το οποίο εκμεταλλεύεται ευπάθειες στο λειτουργικό σύστημα του Android δίνοντας στην κακόβουλη οντότητα δικαιώματα πλήρους πρόσβασης (root) σε παραβιασμένες κινητές συσκευές.

Triada

Modular backdoor για Android που εκχωρεί δικαιώματα super user σε κακόβουλο λογισμικό που έχει ληφθεί, βοηθώντας το να ενσωματωθεί σε διαδικασίες του συστήματος. Το Triada έχει την δυνατότητα επίσης να παραποιεί διευθύνσεις URL που φορτώνονται στο πρόγραμμα περιήγησης.[15]

3.2.9 Αντιμετώπιση κυβερνοεπιθέσεων

Η πρόληψη είναι καλύτερη από τη θεραπεία - αυτή η φράση αποδεικνύεται αληθινή για την αντιμετώπιση των σύγχρονων απειλών ασφαλείας. Συχνά, είναι λιγότερο δαπανηρό να αποτρέψουμε ένα συμβάν ασφαλείας από το να κάνουμε μια ανάλυση μετά την καταστροφή. Μια επίθεση στον κυβερνοχώρο εγγυάται ορισμένα ή όλα τα ακόλουθα βήματα για την πλήρη απογραφή της κατάστασης και των διορθωτικών μέτρων που είναι απαραίτητο να ληφθούν:

- Αξιολόγηση εάν το συμβάν ασφαλείας είναι πραγματικό, ορισμένες επιθέσεις μπορεί να είναι μικρές και να διορθωθούν αμέσως, ενώ άλλες μπορεί να είναι αρκετά μεγάλες και να έχουν πολυάριθμες επιπτώσεις στην υποδομή πληροφορικής ενός οργανισμού. Εάν η επίθεση είναι πραγματική, είναι απαραίτητη η δημιουργία αντιγράφων ασφαλείας δεδομένων (εάν τα δεδομένα είναι προσβάσιμα και δεν έχουν παραβιαστεί). Η διατήρηση των δεδομένων μπορεί να βοηθήσει πολύ σε τέτοιες καταστάσεις.

- Εφαρμογή του προγράμματος συμβάντων, προσαρμοσμένο ανάλογα με τον τύπο της επίθεσης.

- Ενημέρωση του υπευθύνου ασφαλείας ως μέρος του πρωτοκόλλου επικοινωνίας.

- Παρουσίαση των γεγονότων σύμφωνα με το περιστατικό και τις διορθωτικές ενέργειες που σχεδιάζονται για τον έλεγχο της ζημιάς και τα μέτρα για την πρόληψη τέτοιων επιθέσεων στο μέλλον.

Σε ορισμένες περιπτώσεις, οι εσωτερικές επιθέσεις θα μπορούσαν να είναι η πηγή. Σε μια τέτοια περίπτωση, είναι συνετό να ξεκινήσει μια έρευνα και να αναληφθεί κατάλληλη δράση.

Βέλτιστες πρακτικές αντιμετώπισης κυβερνοεπιθέσεων

Αντιμέτωποι με σύνθετες απειλές για την ασφάλεια και νέες τεχνικές επίθεσης, όσο ισχυρή και αν είναι μια εφαρμογή συστήματος / ιστού, δεν είναι ποτέ απόλυτα ασφαλής. Αυτή η γενική πραγματικότητα, ωστόσο, δεν πρέπει να μας αποτρέψει από τη δημιουργία βέλτιστων πρακτικών στον κυβερνοχώρο, οι οποίες λειτουργούν ως η πρώτη γραμμή άμυνας σε περίπτωση ισχυρής επίθεσης στον κυβερνοχώρο.

Είναι αναγκαίο να γίνει αναφορά , στις τεχνικές και τις πολιτικές για την πρόληψη των κυβερνοεπιθέσεων τόσο για χρήστες η υπαλλήλους ενός οργανισμού:

- Χρήση μιας ολοκληρωμένης λύσης προστασίας από ιούς που παρακολουθεί τις διαδικτυακές δραστηριότητες των χρηστών, τους ιστότοπους που επισκέπτονται και τα συνημμένα που ανοίγουν κ.λπ. για την αποφυγή επιθέσεων κακόβουλου λογισμικού.

- Εγκατάσταση τείχους προστασίας.

- Παρακολούθηση του εσωτερικού δικτύου και διερεύνηση για οποιαδήποτε ύποπτη δραστηριότητα ή ενός ανεπιθύμητου περιστατικού. Η επένδυση σε ολοκληρωμένες σουίτες ασφαλείας, όπως το AppSealing, μπορεί να κάνει τη διαφορά στην πρόληψη μιας επίθεσης στον κυβερνοχώρο.

- Ανάπτυξη και εφαρμογή Πολιτικών ασφάλειας που εξασφαλίζουν την ομοιόμορφη εφαρμογή των ελέγχων ασφάλειας δεδομένων στο σύνολο μιας επιχείρησης.

- Προγραμματισμός της τακτικής δημιουργίας αντιγράφων ασφαλείας δεδομένων (συμπεριλαμβανομένων των δεδομένων cloud) ως οργανωτική πρακτική και αποθήκευση του αντίγραφου ασφαλείας σε ξεχωριστό διακομιστή. Αυτή η συνήθεια αποτρέπει την κρίσιμη απώλεια δεδομένων σε περίπτωση επίθεσης στον κυβερνοχώρο, συμπεριλαμβανομένων επιθέσεων ransomware.

- Εφαρμογή ισχυρών και ασφαλών πρακτικών κωδικού πρόσβασης για την αποφυγή παραβιάσεων ασφάλειας, ειδικά με την πρόσβαση πολλών συσκευών σε δεδομένα από δίκτυα εταιρειών. Οι ισχυροί κωδικοί πρόσβασης εξακολουθούν να είναι ένας από τους πιο στοιχειώδεις τρόπους για την ενίσχυση της ασφάλειας στον κυβερνοχώρο για κάθε χρήστη και οργανισμό.

- Συνεργασία με ειδικούς ασφαλείας για να εντοπιστούν κενά σε εφαρμογές προκειμένου να ληφθούν διορθωτικά μέτρα για την αποφυγή μόλυνσης από κακόβουλο λογισμικό/XSS.

Εν ολίγοις, η υιοθέτηση μιας προληπτικής προσέγγισης είναι ο μόνος βιώσιμος τρόπος αντιμετώπισης σύγχρονων σεναρίων απειλών για την ασφάλεια. Αυτή η προσέγγιση πρέπει να δημιουργήσει μια ισχυρή αρχιτεκτονική ασφάλειας που να καλύπτει τόσο τις ανάγκες ασφάλειας δικτύου όσο και εφαρμογών ενός οργανισμού.

3.2.10 Ιστορία των κυβερνοεπιθέσεων

Morris Worm (1988)

Ο Robert Tappan Morris (γεννημένος στις 8 Νοεμβρίου 1965) έγινε γνωστός για τη δημιουργία του Morris Worm το 1988 σε ηλικία 15 ετών, που θεωρείται το πρώτο worm υπολογιστή στο Διαδίκτυο. Ο Morris διώχθηκε για απελευθέρωση του worm και έγινε το πρώτο άτομο που καταδικάστηκε βάσει του τότε νόμου περί απάτης και κατάχρησης υπολογιστών. Το worm στόχευε μόνο υπολογιστές που εκτελούσαν μια συγκεκριμένη έκδοση του λειτουργικού συστήματος Unix, αλλά εξαπλώθηκε ευρέως εκμεταλλευόμενο τις ευπάθειες στο UNIX send mail, finger και rsh/rexec καθώς και μαντεύοντας αδύναμους κωδικούς πρόσβασης. Οι λειτουργίες των τερματικών που μολύνθηκαν επιβραδύνθηκαν ενώ τα email καθυστέρησαν για μέρες. Οι ακριβείς ζημιές ήταν δύσκολο να ποσοτικοποιηθούν, αλλά οι εκτιμήσεις ξεκίνησαν από 100.000$ και αυξήθηκαν σε εκατομμύρια. Αναμφίβολα το Morris worm έπαιξε ρόλο στην έμπνευση των καταστροφικών κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) που υπάρχει σήμερα.[20][21]

Solar Sunrise (1998)

Η επίθεση που αρχικά θεωρήθηκε ότι υπήρξε η προσπάθεια Ιρακινών κυβερνητικών, ξεκίνησε με τη μορφή συστηματικών επιθέσεων στον κυβερνοχώρο των ΗΠΑ, η οποία κατάσχεσε τον έλεγχο πάνω από 500 κυβερνητικών και ιδιωτικών συστημάτων πληροφορικής. Οι επιτιθέμενοι εκμεταλλεύτηκαν μια γνωστή ευπάθεια στο σύστημα υπολογιστών Solaris (που βασίζεται σε UNIX). Είχαν τη δυνατότητα να εκτελέσουν έμμεσα αυθαίρετες εντολές με δικαιώματα superuser χωρίς να απαιτείται τοπική πρόσβαση στον κεντρικό υπολογιστή προορισμού Η κυβέρνηση των ΗΠΑ συγκέντρωσε διάφορα τμήματα άμυνας, συμπεριλαμβανομένου του FBI και του Οργανισμού Πληροφοριακών Συστημάτων Άμυνας, για να διερευνήσουν το θέμα. Μεγάλη έκπληξη για όλους ήταν ότι δεν υπήρχαν Ιρακινοί κυβερνητικού που να εμπλέκονται στην επίθεση. Οι έρευνες όμως οδήγησαν στη σύλληψη τριών εφήβων από την Καλιφόρνια. Οι επιθέσεις υπενθύμισαν στους φορείς πως μια συντονισμένη προσπάθεια θα μπορούσε να επηρεάσει την υποδομή πληροφορικής μιας ολόκληρης χώρας.[22]

Ο ιός Melissa (1999)

Ο ιός Melissa δημιουργήθηκε από τον Αμερικανό David L. Smith και πρωτοεμφανίστηκε στις 26 Μαρτίου 1999 σε μορφή e-mail. Ο ιός βρισκόταν σε ένα αρχείο με όνομα "List.doc", που περιείχε κωδικούς για πρόσβαση σε 80 πορνογραφικές ιστοσελίδες. Η αρχική έκδοση του ιού εστάλη σε πολλαπλούς χρήστες μέσω ηλεκτρονικού ταχυδρομείου. Ο ιός Melissa εξαπλώνεται κυρίως μέσα από προγράμματα του Microsoft Office όπως το Word και το Excel, και έχει την ικανότητα να πολλαπλασιάζει τον εαυτό του στέλνοντας e-mail μέσω προγραμμάτων όπως το Microsoft Outlook ή το Outlook Express. Σε περίπτωση που ένα αρχείο που περιέχει τον ιό ανοιχτεί, εκτελείται μια μακροεντολή η οποία επιλέγει τα πρώτα 50 άτομα από τη λίστα των χρηστών και στην συνέχεια στέλνει σε όλους e-mail. Ο Smith καταδικάστηκε σε 10 χρόνια φυλάκιση, ενώ εξέτισε ποινή 20 μηνών και πρόστιμο 5,000$.[22]

Επίθεση χάκερ στην NASA και υπουργείο άμυνας των ΗΠΑ (1999)

Το 1999 ο Τζόναθαν Τζέιμς σε ηλικία 15 ετών κατάφερε να διεισδύσει στους υπολογιστές ενός τμήματος του Υπουργείου Άμυνας των ΗΠΑ εγκαθιστώντας ένα «backdoor» στους διακομιστές του. Αυτό του επέτρεψε να παρακολουθεί χιλιάδες εσωτερικά μηνύματα ηλεκτρονικού ταχυδρομείου από διάφορες κυβερνητικές οργανώσεις, συμπεριλαμβανομένων εκείνων που περιέχουν ονόματα χρήστη και κωδικούς πρόσβασης για διάφορους στρατιωτικούς υπολογιστές.

Χρησιμοποιώντας τις κλεμμένες πληροφορίες, ο Τζέιμς μπόρεσε να κλέψει ένα κομμάτι λογισμικού της NASA, το οποίο κόστισε στο γραφείο εξερεύνησης του διαστήματος 41.000 δολάρια καθώς τα συστήματα έκλεισαν για τρεις εβδομάδες. Σύμφωνα με τη NASA, «το κόστος του λογισμικού, είχε αξία 1,7 εκατομμύρια δολάρια».[22]

MafiaBoy (2000)

Ο Michael Calce, γνωστός και ως "MafiaBoy", το 2000 και σε ηλικία 15 ετών, πραγματοποίησε μια τεράστια επίθεση άρνησης εξυπηρέτησης (DoS) που κατέλυσε μερικούς από τους πιο δημοφιλείς ιστότοπους του διαδικτύου. Αποκαλώντας την επίθεση Rivolta, που σημαίνει «ταραχή» στα ιταλικά, έριξε το Yahoo , το eBay, το

CNN, το Amazon και άλλους ιστότοπους, προκαλώντας ζημίες περίπου 1,7 δισεκατομμυρίων δολαρίων. Αργότερα συνελήφθη. Επειδή ήταν ακόμα ανήλικος, ο Κάλτσε καταδικάστηκε το 2001 σε οκτώ μήνες υπό ανοικτή κράτηση, πράγμα που σημαίνει ότι οι κινήσεις και οι ενέργειές του θα ήταν περιορισμένες. Η διαδικτυακή του πρόσβαση περιορίστηκε επίσης από το δικαστήριο. Στο ντοκιμαντέρ του, Rivolta: Inside the Mind of the Canada's Notorious Hacker, ο Calce δήλωσε ότι «η πειρατεία συσχετίζεται με ένα ναρκωτικό.»[22][23]

Επιθέσεις στο Διαδίκτυο (2002)

Το 2002, μια επίθεση στον κυβερνοχώρο που στόχευε στους 13 βασικότερους domain name root servers στις ΗΠΑ σχεδόν έθεσε το Διαδίκτυο εκτός λειτουργίας. Ήταν μια επίθεση DDoS που διήρκεσε μία ώρα. Αν και δεν διήρκησε πολύ, ή κλίμακα της επίθεσης ήταν ιδιαιτέρως ανησυχητική. Εκείνη την εποχή, οι ομοσπονδιακές αρχές των ΗΠΑ χαρακτήρισαν την επίθεση ως τη μεγαλύτερη και πιο περίπλοκη στην ιστορία. Οι διακομιστές Διαδικτύου υπέστησαν σοβαρή πίεση για μία ώρα, παρόλο που οι χρήστες πιθανότατα δεν είχαν δυσμενείς επιπτώσεις. Σε περίπτωση που η επιθέσεις διαρκούσαν περισσότερο, το Διαδίκτυο θα έπαυε να λειτουργεί.[22]

Επίθεση στην Ιστοσελίδα της Σαϊεντολογίας (2008)

Τον Ιανουάριο του 2008, ένας έφηβος από το Νιου Τζέρσεϋ μαζί με μια συμμορία χάκερ με το όνομα Annoymous ξεκίνησαν μια επίθεση DDoS που κατέλυσε τον ιστότοπο της Εκκλησίας της Σαϊεντολογίας για αρκετές ημέρες. Το μέλος τον Annoymous Ντμίτρι Γκόζνερ κατηγορήθηκε και καταδικάστηκε για την επίθεση DDoS. Η μέγιστη ποινή ήταν 10 χρόνια φυλάκιση και πρόστιμο 250.000 δολαρίων, αλλά τελικά καταδικάστηκε σε δύο χρόνια δοκιμασία και διέταξε να καταβάλει στην Εκκλησία της Σαϊεντολογίας 37.500 δολάρια.[22]

Μαζική κλοπή στοιχείων πιστωτικών καρτών από χάκερ (2009):

Ο Albert Gonzalez (γεννημένος το 1981) είναι ένας αμερικανός χάκερ, που, με την χρήση μιας SQL injection επίθεσης κατάφερε να αποκτήσει πρόσβαση στο Heartland Payment Systems, μια εταιρεία του Νιου Τζέρσεϋ που επεξεργάζεται πληρωμές από το κατάστημα 7-Eleven και την αλυσίδα σούπερ μάρκετ Hannaford. Αυτό είχε ως αποτέλεσμα περισσότεροι από 40 εκατομμύρια αριθμοί πιστωτικών και χρεωστικών

καρτών να κλαπούν από μεγάλους λιανοπωλητές των Η.Π.Α. ως αποτέλεσμα της επίθεσης. Η απάτη, από τον Οκτώβριο του 2006 έως τον Μάιο του 2008, σηματοδοτεί την τελευταία και μεγαλύτερη σε τουλάχιστον πέντε χρόνια φερόμενης εγκληματικής δραστηριότητας από τον Γκονζάλες. Ο 28χρονος βρίσκεται ήδη στη φυλακή.[22]

Η ραγδαία αύξηση των κυβερνοεπιθέσεων, σε κλίμακα και συχνότητα, καθιστά ζωτικής σημασίας την αντιμετώπιση αντίστοιχων περιστατικών για την προστασία ενός οργανισμού ή ενός χρήστη του διαδικτύου. Η μη αποτελεσματική ανταπόκριση σε ένα τέτοιο περιστατικό, μπορεί όχι μόνο να θέσει σε κίνδυνο σημαντικά και απόρρητα δεδομένα του οργανισμού αλλά και να επιφέρει αρνητικές επιπτώσεις ή ακόμα και ρήξη στην σχέση του οργανισμού με τους πελάτες του. Στην προστασία από ανάλογους κινδύνους, μπορούν να συμβάλουν καθολικά οι μηχανές αναζήτησης κακόβουλου λογισμικού μέσω της τεχνολογίας API που χρησιμοποιούν. Ο εντοπισμός και η ανάλυση ύποπτων αρχείων καθώς και η διεξαγωγή κατάλληλων δοκιμών ασφαλείας μπορούν να διεξάγονται με την χρήση των μηχανών αναζήτησης ώστε να μεγιστοποιείται η ασφάλεια του οργανισμού και των χρηστών του διαδικτύου και να διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων.

4.Εισαγωγή στην API τεχνολογία

Στην σημερινή εποχή αν και οι υπολογιστές γίνονται πιο ασφαλείς με κάθε νέα έκδοση ή ενημέρωση του λειτουργικού συστήματος, οι εισβολείς μπορούν να παρακάμψουν αυτά τα στοιχεία ασφαλείας χρησιμοποιώντας διαφορετικές μεθόδους. Το πιο κοινό σενάριο των μεθόδων παράκαμψης στοιχείων ασφαλείας είναι ότι το κακόβουλο λογισμικό αλλάζει την πηγή του κώδικα και συμπεριφορά σε κάθε μολυσμένο υπολογιστή. Το σύνολο των μεθόδων που χρησιμοποιούνται από τους αναλυτές για τον εντοπισμό κακόβουλου λογισμικού ονομάζεται ανάλυση κακόβουλου λογισμικού. Η ανάλυση κακόβουλου λογισμικού είναι ένας ευρύς όρος και περιλαμβάνει πολλά στάδια. Αυτά τα στάδια περιλαμβάνουν εξέταση του περιεχομένου του ύποπτου λογισμικού χωρίς την εκτέλεσή του και στη συνέχεια εκτέλεση του λογισμικού σε απομονωμένο περιβάλλον, εξέταση των αιτημάτων ανάλυσης domain name (DNS), καταγραφή της register (read/write), και τις προσπελάσεις αρχείων και κλήσεων διεπαφής προγραμματισμού εφαρμογών (API). Για την προστασία από κακόβουλο λογισμικό, πολλά προϊόντα παράγονται τόσο εμπορικά όσο και ακαδημαϊκά. Λαμβάνοντας υπόψη την ανάπτυξη κακόβουλου λογισμικού, παρατηρείται ότι έχουν υποστεί μια δομικά τέλεια εξέλιξη. Η ανίχνευση και η ανάλυση του κακόβουλου λογισμικού κρίνεται αναγκαία.

4.1 Τι είναι το API

Μια διεπαφή προγραμματισμού εφαρμογών (API) είναι ένα σύνολο εργαλείων, ορισμών και πρωτοκόλλων για την ενσωμάτωση λογισμικού και υπηρεσιών εφαρμογών. Είναι η δυνατότητα η οποία επιτρέπει στα προϊόντα και τις υπηρεσίες να επικοινωνούν με άλλα προϊόντα και υπηρεσίες χωρίς να χρειάζεται να δημιουργείτε συνεχώς νέα υποδομή σύνδεσης. Τα API μπορούν να είναι ιδιωτικά (μόνο για εσωτερική χρήση), να συνεργάζονται (να κοινοποιούνται σε συγκεκριμένους συνεργάτες για την παροχή πρόσθετων ροών εσόδων) ή να είναι δημόσια (επιτρέποντας σε τρίτα μέρη να αναπτύξουν εφαρμογές που αλληλεπιδρούν με το API για την προώθηση της καινοτομίας). Η επιλογή κοινής χρήσης των API έχει πολλά οφέλη, όπως:

- Δημιουργία νέων καναλιών εσόδων ή επέκταση υπαρχόντων.
- Επέκταση της εμβέλειας του Brand.

- Διευκόλυνση ανοικτής καινοτομίας ή βελτιωμένη αποτελεσματικότητα μέσω εξωτερικής ανάπτυξης και συνεργασίας.

Τα APIs κατασκευάζονται χρησιμοποιώντας είτε το REpresentational state transfer (REST), μία αρχιτεκτονική για την ανάπτυξη διαδικτυακών υπηρεσιών που είναι δημοφιλής λόγω της απλότητάς του ή του απλού πρωτοκόλλου πρόσβασης αντικειμένου (SOAP-simple object access protocol), που επιτρέπει την επικοινωνία κατανεμημένων στοιχείων μιας εφαρμογής. Το SOAP μπορεί να μεταφερθεί σε μια ποικιλία πρωτοκόλλων χαμηλότερου επιπέδου, συμπεριλαμβανομένου του πρωτοκόλλου μεταφοράς υπερκειμένου (HTTP) που σχετίζεται με τον ιστό. Τα REST APIs χρησιμοποιούν HTTP και μεταφορά επιπέδου ασφαλείας TLS. Χρησιμοποιούν επίσης Javascript Object Notation (JSON), μια μορφή ανταλλαγής δεδομένων που βασίζεται σε κείμενο, αναγνώσιμη από τον άνθρωπο και χρησιμοποιείται για την αναπαράσταση απλών δομών δεδομένων και αντικειμένων σε κώδικα που βασίζεται στο πρόγραμμα περιήγησης στο Web.[24]

4.2 Χρήσεις της API τεχνολογίας

Τα APIs αφορούν την ενοποίηση-σύνδεση δεδομένων, εφαρμογών και συσκευών σε έναν οργανισμό, έτσι ώστε όλες οι τεχνολογίες να μπορούν να επικοινωνούν και να συνεργάζονται καλύτερα. Μαζί με την κατανεμημένη ενσωμάτωση, αποτελούν βασικό χαρακτηριστικό της ευέλικτης ενοποίησης. Η ευέλικτη ενσωμάτωση είναι μια αρχιτεκτονική προσέγγιση στην πλατφόρμα ενοποίησης που δίνει έμφαση σε ένα μικρό IT footprint το οποίο είναι εξαιρετικά επεκτάσιμο και διαθέσιμο και έχει καλά καθορισμένα επαναχρησιμοποιήσιμα και διαχειριζόμενα τελικά σημεία.

4.3 Η αναγκαιότητα της χρήσης των APIs στην ασφάλεια

Οι κυβερνοεπιθέσεις αυξάνονται, ιδίως μέσω της χρήσης παραβιασμένων ταυτοτήτων και APIs. Ορισμένες επιθέσεις που θα μπορούσαν να επιβληθούν σε APIs περιλαμβάνουν: επιθέσεις MITM, επιθέσεις παραμέτρων και επιθέσεις ταυτότητας. Ως αποτέλεσμα, πολλοί από τους μεγαλύτερους παρόχους υπηρεσιών διαδικτύου απαιτούν από τους συνεργάτες τους να αυξήσουν τα μέτρα ασφαλείας, συμπεριλαμβανομένης της χρήσης MFA (multi factor authentication), ενός συστήματος ασφαλείας που απαιτεί περισσότερες από μία μεθόδους ελέγχου ταυτότητας από ανεξάρτητες κατηγορίες διαπιστευτηρίων για την επαλήθευση της ταυτότητας του χρήστη για σύνδεση ή άλλη συναλλαγή. Τέτοιοι πάροχοι υπηρεσιών περιλαμβάνουν την Amazon και τη Microsoft,

οι οποίες τον Αύγουστο του 2019 άρχισαν να απαιτούν από τους συνεργάτες του προγράμματος παροχής λύσεων cloud, την επιβολή MFA για κάθε χρήστη.

Η εφαρμογή της ασφάλειας API είναι σημαντική επειδή μπορεί να αποτρέψει XSS και SQL injection επιθέσεις, καθώς και να παρέχει προστασία σε πιθανές παραβιάσεις ευαίσθητων δεδομένων. Συνολικά, η ασφάλεια API είναι ζωτικής σημασίας για την επιτυχή και ασφαλή απόδοση αυτών, αλλά και των προγραμμάτων που υποστηρίζουν.[25]

4.4 Η λειτουργία των API στην ασφάλεια

Η ασφάλεια API βασίζεται σε μεγάλο βαθμό στον έλεγχο ταυτότητας και την εξουσιοδότηση, με το πρώτο να αποτελεί το αρχικό βήμα στην ασφάλεια API. Ο έλεγχος ταυτότητας αναφέρεται στην επαλήθευση ότι η εφαρμογή πελάτη διαθέτει ασφαλή ταυτότητα και επιτρέπεται να χρησιμοποιεί το API. Η εξουσιοδότηση είναι ένα επόμενο βήμα που περιλαμβάνει τον προσδιορισμό των δεδομένων και των ενεργειών στις οποίες μπορεί να έχει πρόσβαση μια επικυρωμένη εφαρμογή ενώ αλληλεπιδρά με το API. Εκτός από την ορθή εφαρμογή ενός ασφαλούς συστήματος ελέγχου ταυτότητας και εξουσιοδότησης, τα APIs πρέπει να αναπτυχθούν με άλλα προστατευτικά χαρακτηριστικά για να μειωθεί η ευπάθεια του συστήματος σε κακόβουλες επιθέσεις κατά τη διάρκεια κλήσεων API.

Ο προγραμματιστής είναι υπεύθυνος για να διασφαλίσει ότι το κατασκευασμένο API επικυρώνει επιτυχώς όλες τις εισροές από χρήστες που συλλέγονται κατά τη διάρκεια των κλήσεων. Η χρήση των προετοιμασμένων δηλώσεων με μεταβλητές δέσμευσης είναι ένας από τους πιο αποτελεσματικούς τρόπους για την προστασία του API από την SQL injection. Η γλώσσα που χρησιμοποιείται για τη σύνταξη του API περιέχει συχνά λειτουργίες που μπορούν να βοηθήσουν σε αυτό το μέτρο ασφαλείας. Το XSS μπορεί να αντιμετωπιστεί εφικτά καθαρίζοντας την είσοδο χρήστη από την κλήση API. Καθαρίζοντας την είσοδο, οι ετικέτες HTML και JavaScript διαγράφονται και ελαχιστοποιούνται οι πιθανές ευπάθειες XSS.Το Throttling είναι επίσης μια αποτελεσματική πρακτική ασφάλειας API επειδή επιτρέπει τη διαχείριση και τον περιορισμό της πρόσβασης ενός πελάτη σε δεδομένα. Μέσω της χρήσης περιορισμού, οι παρατυπίες στη χρήση του API από τον πελάτη μπορούν να μετρηθούν και έτσι δημιουργείται ένα επιπλέον επίπεδο ασφάλειας μεταξύ του πελάτη και των ευαίσθητων δεδομένων.

5. Μηχανισμοί ανίχνευσης κακόβουλου λογισμικού

5.1 Virus_total

Το VirusTotal είναι ένας ιστότοπος που δημιουργήθηκε από την ισπανική εταιρεία ασφαλείας Hispasec Sistemas. Ξεκίνησε τη λειτουργία του τον Ιούνιο του 2004, ενώ εξαγοράστηκε από την Google Inc τον Σεπτέμβριο του 2012. Η ιδιοκτησία της εταιρείας άλλαξε τον Ιανουάριο του 2018 και πλέον αποτελεί μια από τις θυγατρικές εταιρίες της Alphabet Inc. Το VirusTotal είναι ένα δωρεάν εργαλείο το οποίο ο χρήστης μπορεί να εγκαταστήσει σε επιτραπέζιο υπολογιστή ή να έχει πρόσβαση σε αυτό μέσω διαδικτύου. Χρησιμοποιείται για την ανάλυση ύποπτων αρχείων, hashes ή διευθύνσεων URL, και για τη διευκόλυνση της ανίχνευσης διαφορετικών τύπων κακόβουλου λογισμικού, συμπεριλαμβανομένων ιών, worms και trojans. Για την ανάλυση και τον εντοπισμό τυχόν κακόβουλου περιεχόμενου διαθέσιμο σε διευθύνσεις Ip/Url ή αρχεία το virus total χρησιμοποιεί έναν αριθμό από Antivirus καθώς και σαρωτές ιστότοπων για την εύρεση malware.

Πιο συγκεκριμένα, το VirusTotal χρησιμοποιεί 58 προϊόντα προστασίας από ιούς, όπως το Kaspersky Lab, Doctor, AVG Technologies, Cyren, περισσότερες από 62 Website/domain μηχανές σάρωσης και datasets όπως το AutoShun, CRDF, Sucuri SiteCheck, Quttera καθώς και περισσότερα από 18 εργαλεία για το χαρακτηρισμό αρχείων όπως ExifTool, Snort και Wireshark. Το VirusTotal συγκεντρώνει πολλά προϊόντα προστασίας από ιούς και μηχανές σάρωσης στο διαδίκτυο για να ελέγξει για ιούς που ενδέχεται να έχουν διαφύγει του λογισμικού προστασίας από ιούς ή για να επαληθεύσει τυχόν ψευδός θετικά. Αρχεία μεγέθους έως 550 MB μπορούν να μεταφορτωθούν στον ιστότοπο ή να σταλούν μέσω email (μέγιστο μέγεθος έως 32 MB). Το VirusTotal χρησιμοποιείται ευρέως από την ερευνητική κοινότητα για data labeling ή αξιολόγηση ενός συστήματος. Για παράδειγμα, εάν ένας συγκεκριμένος αριθμός προμηθευτών επισημαίνει ένα αρχείο/διεύθυνση URL ως «Κακόβουλο», οι ερευνητές θα αποδεχθούν ότι το αρχείο περιέχει κακόβουλο λογισμικό. Δυστυχώς, το VirusTotal λειτουργεί σαν ένα μαύρο κουτί και δεν είναι κατανοητό πώς δημιουργεί τις ετικέτες για μια δεδομένη διεύθυνση URL ή αρχείο. Αυτό οδηγεί σε κρίσιμα ερωτήματα: για το αν τα αποτελέσματα του είναι αξιόπιστα αν οι ερευνητές χρησιμοποιούν το VirusTotal με τον σωστό τρόπο.

Προκειμένου να δοθεί απάντηση λάβαμε υπόψη την πειραματική διαδικασία που ακολούθησε μια ερευνητική ομάδα δημιουργώντας μια σειρά από ιστότοπους ηλεκτρονικού ψαρέματος (phishing) υποβάλλοντας τα αντίστοιχα Url ηλεκτρονικού ψαρέματος σε διάφορα API σάρωσης για την εύρεση κακόβουλου λογισμικού. Στην συνέχεια παράλληλα με την συλλογή των logs της εισερχόμενης κίνησης δικτύου για τους phising ιστότοπους υποβάλλονταν ερωτήσεις για αυτές τις διευθύνσεις Url από το VirusTotal για το χρονικό διάστημα ενός μήνα μήνα. Σε συνολικό αριθμό 66 πειραματικών ιστότοπων αναζήτησης βρέθηκαν τα παρακάτω αποτελέσματα.

• Πρώτον, οι περισσότεροι προμηθευτές (vendors) δυσκολεύτηκαν να εντοπίσουν τους απλούς ιστότοπους ηλεκτρονικού ψαρέματος που είχαν δημιουργηθεί. Κατόπιν πολλαπλών σαρώσεων, μόνο 15 προμηθευτές από τους 68 κατάφεραν να εντοπίσουν τουλάχιστον έναν από τους 36 phishing ιστότοπους ενώ ο καλύτερος προμηθευτής εντόπισε μόνο 26 απλούς ιστότοπους ηλεκτρονικού «ψαρέματος».

• Δεύτερον, η απόδοση ανίχνευσης είναι δραστικά διαφορετική για διαφορετικούς ιστότοπους ηλεκτρονικού ψαρέματος. Οι ιστότοποι PayPal, ως δημοφιλείς στόχοι του ηλεκτρονικού ψαρέματος (phishing), μπορούν να εντοπιστούν γρήγορα σε περισσότερους από 10 προμηθευτές κατά την πρώτη σάρωση. Ωστόσο, κανένας από τους 68 προμηθευτές που χρησιμοποιούν μόνο API σάρωσης ιού δεν μπόρεσαν να εντοπίσουν λιγότερο γνωστούς ιστότοπους .

• Τρίτον, τα αποτελέσματα σάρωσης των προμηθευτών δεν ενημερώνουν το VirusTotal αμέσως μετά την ολοκλήρωση της σάρωσης. Η καθυστέρηση προκαλείται από το γεγονός ότι το VirusTotal τραβά μόνο τα προηγούμενα αποτελέσματα σάρωσης όταν υποβάλλεται ένα νέο αίτημα σάρωσης για την ίδια διεύθυνση Url. Ένας χρήστης που απλά καλεί το query/report/API δεν θα λάβει τα ενημερωμένα αποτελέσματα σάρωσης.

•Τέταρτον, το VirusTotal έχει ασυνεπή αποτελέσματα με τα API σάρωσης των προμηθευτών. Το αποτέλεσμα δείχνει ότι οι τρίτοι προμηθευτές δεν δίνουν πάντα στο VirusTotal την άδεια σάρωσης ή τις πιο ενημερωμένες μαύρες λίστες (blacklist).

Το VirusTotal επιλέχθηκε από το PC World ως ένα από τα καλύτερα 100 προϊόντα του 2007. [26][27][28]

5.2 AbuseIPDB

Το AbuseIPDB αποτελεί μια βάση δεδομένων αφιερωμένη στο να βοηθά τους διαχειριστές συστημάτων να ελέγχουν και να αναφέρουν διευθύνσεις Ip που εμπλέκονται σε κακόβουλη δραστηριότητα, όπως ανεπιθύμητη αλληλογραφία, απόπειρες εισβολής, επιθέσεις DdoS κ.λπ. Για την AbuseIPDB, θεωρείτε κακόβουλη κάθε παράνομη, καταχρηστική ή ακατάλληλη δραστηριότητα που εντοπίστηκε σε μια διεύθυνση Ip, όπως απόπειρα DdoS, κάθε είδους ανεπιθύμητο περιεχόμενο, απόπειρες εισβολής, phishing, πλαστογράφηση, SQL injection κα.

Το AbuseIPDB ενημερώνει την βάση του λαμβάνοντας αναφορές για Ip οι οποίες έχουν καταχωρηθεί σε μαύρη λίστα, μια μέθοδο που χρησιμοποιείται για το φιλτράρισμα παράνομων ή κακόβουλων διευθύνσεων Ip.

Η χρήση της βάσης του AbuseIPDB είναι δωρεάν για τους χρήστες λόγω περιορισμένων πόρων συνεπώς η δυνατότητα αναζήτησης είναι περιορισμένη και ανέρχεται στα 1.000 αιτήματα την ημέρα τόσο για έλεγχο Ip όσο και για ενέργειες αναφοράς μέσω του δωρεάν API, ενώ για webmasters στα 3.000 αιτήματα / ημέρα. Τέλος, για τους υποστηρικτές οι οποίοι στηρίζουν οικονομικά τη λειτουργία του AbuseIPDB ανέρχεται στα 5.000 αιτήματα / ημέρα.

Το AbuseIPDB παρέχει δωρεάν API για τον έλεγχο και την αναφορά διευθύνσεων IP, που μπορούν να χρησιμοποιηθούν για ενοποίηση με οποιονδήποτε ιστότοπο ή εφαρμογή. Για να υπολογίσει κατά πόσο μια διεύθυνση Ip είναι κακόβουλη χρησιμοποιεί (κλίμακα 0-100) και με βάση τις αναφορές χρηστών κρίνει κατά πόσο μια διεύθυνση Ip είναι κακόβουλη ή όχι. Εφόσον η βαθμολογία είναι 100 αυτό συνεπάγεται ότι μια διεύθυνση Ip είναι κακόβουλη, ενώ η βαθμολογία 0 σημαίνει ότι δεν συντρέχει κανένας λόγος ανησυχίας για τη φήμη της προαναφερθείσας διεύθυνσης. Για το λόγο ότι η βαθμολογία εμπιστοσύνης των χρηστών αποτελεί μια καθαρά υποκειμενική έννοια και επειδή αυτή η μέτρηση μπορεί να χρησιμοποιηθεί ως βάση για τον αποκλεισμό συνδέσεων, η Abuse IPDB φροντίζει να θεωρεί ως κακόβουλες μόνο τις διευθύνσεις τις οποίες έχουν ήδη χαρακτηριστεί αρνητικά από έναν ισχυρό αριθμό χρηστών του AbuseIPDB.

Η βαθμολογία εμπιστοσύνης καθορίζεται από τις αναφορές και την ηλικία τους. Η βασική τιμή είναι η φυσική λογαριθμική τιμή διακριτών αναφορών χρηστών σε

συνδυασμό με τη λογαριθμική τιμή διακριτών ανώνυμων αναφορών. Οι ανώνυμοι χρήστες που κάνουν report έχουν μειωμένο βάρος. Όλα τα βάρη αναφοράς διαγράφονται με το χρόνο. Οι αξιολογήσεις εμπιστοσύνης για όλες τις αναφερόμενες διευθύνσεις υπολογίζονται εκ νέου καθημερινά. Ορισμένα χαρακτηριστικά χρήστη μπορούν επίσης να αυξήσουν ελαφρώς το βάρος, όπως το αν οι χρήστες ανήκουν στην κλάση του webmaster ή του supporter. Ο τρόπος υπολογισμού έχει σχεδιαστεί πολύ προσεκτικά για να διασφαλίσει ότι κανένας reporter δεν μπορεί να υπερνικήσει τις βαθμολογίες και παρά μόνο από τη συνεργασία μπορεί να οικοδομηθεί ένα αποτελεσματικό δίχτυ εμπιστοσύνης.[29]

5.3 IBM® X-Force Exchange

Το IBM® X-Force Exchange είναι μια cloud-based πλατφόρμα ανταλλαγής πληροφοριών για απειλές και μπορεί να χρησιμοποιηθεί για την γρήγορη έρευνα των πιο πρόσφατων παγκόσμιων απειλών για την ασφάλεια, την συγκέντρωση πληροφοριών και την συμβουλή από ειδικούς ασφάλειας. Το XFE προορίζεται πρωτίστως για αναλυτές ασφαλείας, αλλά και οποιοδήποτε στον προαναφερθέντα χώρο, συμπεριλαμβανομένων μελών ενός κέντρου επιχειρήσεων ασφαλείας (SOC), φορέων ασφαλείας δικτύου, διαχειριστών ασφαλείας και Chief Security Officers. Το XFE είναι ένα δωρεάν προϊόν SecaaS (Security-as-a-service) που μπορεί να χρησιμοποιηθεί για να γίνει αναζήτηση της πληροφορίας σχετικά με απειλές, αλλά και για την συλλογή ευρημάτων και τον διαμοιρασμό των πληροφοριών με άλλα μέλη της κοινότητας XFE. Μέσω του XFE μπορεί να πραγματοποιηθεί αναζήτηση διευθύνσεων IPv4 και IPv6, Url, ευπαθειών, ονομάτων εφαρμογών, και κατακερματισμούς MD5. Τέλος υπάρχει η δυνατότητα ομαδοποίησης των αποτελεσμάτων αναζήτησης ανά κατηγορία.

Οι πληροφορίες που παρέχονται από την X-Force για οποιονδήποτε τύπο αναζήτησης, οι οποίες επιστρέφονται σε μια «αναφορά», προέρχονται από την εσωτερική της υποδομή και βάσεις δεδομένων, καθώς και από περιεχόμενο ανοιχτού κώδικα και συνεργασίες τρίτων μερών για την αύξηση του αριθμού αυτών των πληροφοριών. Το X-Force παρέχει βαθμολογία κινδύνου, τοποθεσία, πληροφορίες κατηγοριοποίησης, ιστορικό περιεχόμενο, πληροφορίες και παθητικές DNS για Ip. Συγκεκριμένα, η βαθμολογία κινδύνου βαθμολογείται από 1 έως 10, με το 1 να δείχνει ότι δεν υπάρχει κάποιος κίνδυνος και το 10 να υποδεικνύει το υψηλότερο επίπεδο κινδύνου. Η

βαθμολογία κινδύνου είναι μια ομαλοποιημένη τιμή που παράγεται από την επεξεργασία των πληροφοριών σχετικά με την απειλή, που διατίθενται στην IBM, συμπεριλαμβανομένων των σαρώσεων μέσω Διαδικτύου και της συλλογής ανεπιθύμητων μηνυμάτων από όλο τον κόσμο. Σε υψηλό επίπεδο, αυτή η βαθμολογία αντικατοπτρίζει το μέγεθος του κινδύνου.

Για παράδειγμα, μια Ip που αναγνωρίζεται ως οντότητα αποστολής μεγάλου όγκου ανεπιθύμητων μηνυμάτων έχει συχνά βαθμολογία υψηλού κινδύνου. Αυτή η βαθμολογία μειώνεται με την πάροδο του χρόνου, εάν η Ip καθίσταται λιγότερο ενεργή στην έξοδο ανεπιθύμητων μηνυμάτων, είτε κατ 'όγκο, είτε κατά συχνότητα. Οι πληροφορίες για τις διευθύνσεις Url περιέχουν βαθμολογία κινδύνου, τμηματοποίηση σε μία από τις 75 κατηγορίες, πληροφορίες και παθητικές πληροφορίες DNS. Οι πληροφορίες ευπάθειας προέρχονται από την X-Force, μια από τις παλαιότερες, διαθέσιμες στο κοινό βάσεις δεδομένων ευπάθειας στον κόσμο. Η βάση δεδομένων περιέχει επί του παρόντος περισσότερες από 88.000 ευπάθειες. Εκτός από τις τυπικές μετρήσεις που σχετίζονται με οποιαδήποτε ευπάθεια, το XFE παρέχει πληροφορίες υποστηριζόμενο από την IBM, η οποία μέσω ενός ολοκληρωμένου χαρτοφυλακίου ασφαλείας ελαχιστοποιώντας τους κινδύνους παρέχει πληροφορίες, για εξωτερικές αναφορές που σχετίζονται με την ευπάθεια. Οι πληροφορίες της εφαρμογής ιστού περιέχουν βαθμολογία κινδύνου, κατηγορίες, σχετικές ενέργειες, βασική διεύθυνση Url και κινδύνους. Περιέχουν επίσης σχετικές πληροφορίες σχετικά με την εφαρμογή, συμπεριλαμβανομένων τρωτών σημείων, διευθύνσεων Url φιλοξενίας και φιλοξενίας Ip. Για τον προσδιορισμό των βαθμολογιών κινδύνου Ip και Url, το X-Force Exchange βασίζεται σε δύο στοιχεία δεδομένων: το ποσό των καταγεγραμμένων αποδεικτικών στοιχείων και το χρονοδιάγραμμα των αποδεικτικών στοιχείων. Ο μηχανισμός ανάλυσης υποστήριξης επεξεργάζεται αυτά τα δεδομένα για να προσδιορίσει τη βαθμολογία κινδύνου.

6. Απαιτήσεις εφαρμογής

Στο κεφάλαιο αυτό αναλύονται οι απαιτήσεις λειτουργίας της εφαρμογής ενώ παράλληλα γίνεται αναφορά στις ειδικές απαιτήσεις και χαρακτηριστικά. Η τελική υλοποίησή της θα πρέπει να προσφέρει ευχρηστία, λειτουργικότητα και αξιοπιστία, προκειμένου ο χρήστης να εμπιστεύεται τα αποτελέσματά της.

Οι απαιτήσεις που ζητήθηκαν για την εφαρμογή μπορούν να συνοψιστούν ως εξής:

1) Δημιουργία εφαρμογής για συσκευές κινητής τηλεφωνίας
2) Πεδίο αναζήτησης δίνοντας την δυνατότητα στον χρήστη να καταχωρήσει Ip/Url προς διερεύνηση
3) Πραγματοποίηση requests (αιτήματα) σε επιλεγμένα API
4) Εμφάνιση των responses (απαντήσεων) του προηγούμενου βήματος
5) Επιλογή πληροφοριών που επιθυμεί ο χρήστης να διατηρήσει
6) Επεξεργασία των πληροφοριών του προηγούμενου βήματος
7) Μετατροπή των επιμέρους αποτελεσμάτων σε κοινή κλίμακα
8) Κατηγοριοποίηση κλίμακας αποτελέσματος (High,Medium,Low)
9) Εξαγωγή αποτελεσμάτων για κάθε API
10) Εξαγωγή τελικού αποτελέσματος (έχει οριστεί το μεγαλύτερο από τα αποτελέσματα των τριών API)
11) Διατήρηση και εμφάνιση ιστορικού αναζητήσεων για το Session (τρέχουσα συνεδρία)
12) Δυνατότητα διασύνδεσης μέσω της εφαρμογής με τις τρείς μηχανές αναζήτησης
13) Πρόσβαση σε γενικές πληροφορίες των τριών μηχανών αναζήτησης (Virus total, AbuseIPDB, Xforce)

6.1 Μεθοδολογία και ροή εφαρμογής

Όπως έχει αναφερθεί, ο σκοπός της παρούσας μεταδιπλωματικής εργασίας είναι η ανάπτυξη μιας εφαρμογής που θα επιτρέπει στον χρήστη με την βοήθεια της τεχνολογίας των APIs να υπολογίζει το συνολικό βαθμό επικινδυνότητας ενός Url ή μίας διεύθυνσης Ip. Για τις ανάγκες της εφαρμογής επιλέχθηκε το MULTI-PLATFORM FRAMEWORK KIVY.

Το Kivy είναι ένα framework για την Python, το οποίο προσφέρει τη δυνατότητα δημιουργίας διαπλατφορμικών και multi-touch εφαρμογών. Ο προγραμματισμός σε Kivy δε διαφέρει από αυτόν σε γλώσσα Python. Παρόλα αυτά το Kivy framework προσφέρει τη δυνατότητα χρήσης της Kivy Language σε περίπτωση που ο χρήστης το επιθυμεί.[32] Στην εφαρμογή, ανάλογα με τα παραγόμενα αποτελέσματα έχει οριστεί για κάθε Alert η κλίμακα αξιολόγησης (High ,Medium,Low) όπως φαίνεται στον παρακάτω πίνακα.

Κατηγορίες Alert βάση αποτελέσματος

Alert	high	medium	low
COLOUR			
RESULT	> 6,7	>3,4	<3,4

Πιο συγκεκριμένα εάν το αποτέλεσμα σε κάποια από τις μηχανές αναζήτησης είναι μεγαλύτερο ή ίσο του 6,7 το Alert θεωρείται«High» και το προβαλλόμενο αποτέλεσμα θα έχει κόκκινο χρώμα. Αντίστοιχα εάν είναι μεγαλύτερο η ίσο από 3,4 έως 6,7 το Alert θα είναι «Medium» και το προβαλλόμενο αποτέλεσμα θα έχει κίτρινο χρώμα. Τέλος εάν είναι 0 έως 3,3 το Alert θεωρείται «Low» και το προβαλλόμενο αποτέλεσμα θα έχει πράσινο χρώμα.

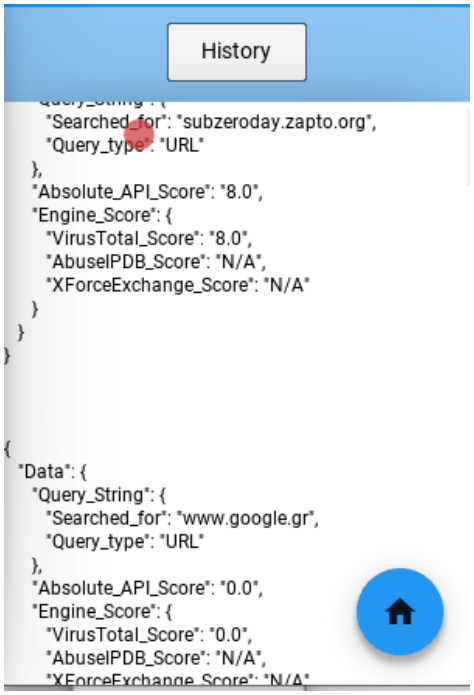
Αρχικά, ο χρήστης κάνει είσοδο στην εφαρμογή. Στην κεντρική οθόνη της εφαρμογής έχει τη δυνατότητα, στο πεδίο αναζήτησης, να καταγράψει την Ip/Url την οποία επιθυμεί να αναζητήσει. Με το πάτημα του πλήκτρου αναζήτησης το πρόγραμμα θα προχωρήσει σε έλεγχο των δεδομένων που έχει εισάγει και εφόσον η καταχώρηση είναι λανθασμένη θα λάβει μήνυμα μη αποδεκτής εισόδου (N/A). Αν, από την άλλη, τα δεδομένα είναι έγκυρα, πραγματοποιείται έλεγχος για το αν η είσοδος του χρήστη αφορά διεύθυνση Ip ή Url και στη συνέχεια πραγματοποιούνται τα αντίστοιχα requests, γίνεται η ανάλυση τους και ο χρήστης λαμβάνει το τελικό score από το κάθε

API. Το virus total όπως έχει ήδη αναφερθεί για την ανάλυση και τον εντοπισμό κακόβουλου περιεχόμενου χρησιμοποιεί Antivirus μηχανές και σαρωτές ιστότοπων. Τα αποτελέσματα ορίζονται σύμφωνα με το συνολικό αριθμό των μηχανών που θα αξιολογήσουν την Ip ή το Url ως κακόβουλο. Το AbuseIpdb με βάση τις αναφορές των χρηστών για να υπολογίσει κατά πόσο μια διεύθυνση Ip είναι κακόβουλη χρησιμοποιεί (κλίμακα 0-100), ενώ για το X-Force η βαθμολογία κινδύνου αξιολογείται από 1 έως 10.

Για τις ανάγκες της εφαρμογής και για την αξιολόγηση των αποτελεσμάτων χρησιμοποιείται ειδικός αλγόριθμος μετατροπής αυτών σε κοινή κλίμακα του 10. Προκειμένου να επιτευχθεί η παραπάνω συνθήκη για το Virus total, το τελικό score υπολογίζεται από τον εξής τύπο: **finalRisk =[(malicious * 10) + (suspicious * 5)]/10** με ανώτατο score το 100. Σε περιπτώσεις μεγαλύτερου Score ο κώδικας μετατρέπει το αποτέλεσμα αυτόματα σε 100. Στον παραπάνω τύπο πολλαπλασιάζουμε τις ανιχνεύσεις αρχείων που έχουν χαρακτηριστεί από τις μηχανές σάρωσης του virus total ως malicious επί δέκα (10) και τις ανιχνεύσεις που έχουν που έχουν χαρακτηριστεί από τις μηχανές σάρωσης ως suspicious επί πέντε (5), με γνώμονα την βαρύτητα της κάθε κατηγορίας. Στην συνέχεια διαιρούμε το αποτέλεσμα με το 10 διατηρώντας ένα δεκαδικό ψηφίο : **score = round((value/10),1**. Από τα επιμέρους αποτελέσματα των τριών μηχανών αναζήτησης διατηρείται το μεγαλύτερο score από τις τρείς μηχανές ως τελικό και εμφανίζεται σε ξεχωριστό πεδίο. Τέλος ο χρήστης μέσω της επιλογής history έχει τη δυνατότητα να λάβει αναλυτικές πληροφορίες σχετικά με τα δεδομένα που είχε εισάγει σε προηγούμενες αναζητήσεις καθώς επίσης τα ενδιάμεσα και τελικά αποτελέσματα των επιμέρους API .

History button

Ο χρήστης, επιλέγοντας το history button από το menu bar στα αριστερά, έχει την δυνατότητα να αναζητήσει πληροφορίες σχετικές με τα αποτελέσματα τελευταίων αναζητήσεων.



7. Συμπεράσματα

Τη σημερινή εποχή το διαδίκτυο αποτελεί το σημαντικότερο μέσο ενημέρωσης παρέχοντας μια πληθώρα από εργαλεία διαφορετικών δυνατοτήτων. Επιτρέπει την ανταλλαγή μεγάλων αρχείων ηλεκτρονικής μορφής, την αναζήτηση υλικού και πληροφοριών, καθώς και την επικοινωνία με πλήθος άλλων ανθρώπων. Ωστόσο, το διαδίκτυο δεν είναι απόλυτα ασφαλές καθώς οι χρήστες του απειλούνται από διάφορους τύπους επιθέσεων όπως ιούς υπολογιστών και κακόβουλο λογισμικό.

Κακόβουλοι χρήστες, εκμεταλλευόμενοι τις ευπάθειες τόσο του χρησιμοποιούμενου λογισμικού και υλικού όσο και τις αδυναμίες των χρηστών, προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, επιχειρώντας να αποκομίσουν κέρδος ή να επηρεάσουν κακοβούλως την λειτουργία των συστημάτων. Υπάρχει λοιπόν η ανάγκη οι χρήστες του διαδικτύου να ακολουθούν μεθόδους και τεχνικές, με τις οποίες θα διαφυλάξουν και θα προστατέψουν τα συστήματα τους.

Σκοπός της παρούσας Διπλωματικής Εργασίας ήταν η διερεύνηση των κινδύνων και η ανάπτυξη μηχανισμού προστασίας από αυτούς. Για το λόγο αυτό υλοποιήθηκε μια mobile εφαρμογή η οποία έχει ως καινοτομία την ανίχνευση και αξιολόγηση της φήμης των διευθύνσεων Url / Ip χρησιμοποιώντας ταυτόχρονα διαφορετικές μηχανές ανίχνευσης και ανάλυσης, τις VirusTotal, XFE και AbuseIPDB.

Εργαλεία όπως τα VirusTotal, AbuseIPDB, XFE, τα οποία χρησιμοποιούν μηχανισμούς σάρωσης, αποτελούν μια από τις βασικές τεχνικές αναγνώρισης και εντοπισμού κινδύνου μέσω αναζήτησης Url ή Ip για την εύρεση κακόβουλου λογισμικού, κάνοντας την περιήγηση του χρήστη πιο ασφαλή. Ο χρήστης παράλληλα μπορεί να αποκτήσει πρόσβαση και να επεξεργαστεί τις απαντήσεις τού κάθε επιμέρους API, ενώ μέσω της επιλογής history έχει τη δυνατότητα να λάβει αναλυτικές πληροφορίες σχετικά με τα δεδομένα που είχε εισάγει σε προηγούμενες αναζητήσεις καθώς επίσης τα ενδιάμεσα και τελικά αποτελέσματα των επιμέρους API. Συνεπώς η δυνατότητα της εφαρμογής να παρέχει συνδυαστικά αποτελέσματα οδηγούν τους χρήστες σε ασφαλέστερα συμπεράσματα εάν μια Ip ή μια διεύθυνση Url είναι κακόβουλη ή όχι και μπορεί να αποτελέσει ένα πολύ χρήσιμο εργαλείο στα χέρια των χρηστών για την αντιμετώπιση των απειλών.

Μελλοντικά προτείνεται περαιτέρω έρευνα για την ανάπτυξη εργαλείων προστασίας τα οποία θα διατίθενται δωρεάν στους χρήστες. Η μεγαλύτερη πρόκληση στην ασφάλεια του διαδικτύου είναι η ανάπτυξη μεθόδων που θα μπορούν να προσφέρουν συνεχώς ενημερωμένες εκδόσεις αυτών των εργαλείων για την αποτελεσματικότερη αντιμετώπιση οποιασδήποτε απειλής.

Βιβλιογραφικές αναφορές

1. What is the OSI Model? https://www.forcepoint.com/cyber-edu/osi-model
2. Parts of the IPv4 Address (System Administration Guide: IP Services) https://docs.oracle.com/cd/E19683-01/806-4075/ipref-1/index.html
3. What Is aURL?https://www.cis.upenn.edu/~bcpierce/courses/629/papers/Java-tutorial/networking/urls/definition.html
4. What is ICMP? | Internet Control Message Protocol | Cloudflare https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/
5. Cybercriminals/ Cybercriminals - Definition - Trend Micro https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals
6. Jason Andress, Steve Winterfeld, in Cyber Warfare (Second Edition), 2014. Hacktivists https://www.sciencedirect.com/topics/computer-science/hacktivists
7. Ransomware - What is it & how to remove it? | Malwarebytes https://www.malwarebytes.com/ransomware/
8. What is a Computer Virus? - Definition from WhatIs.com https://searchsecurity.techtarget.com/definition/virus
9. Συνήθεις ερωτήσεις σχετικά με ιούς μακροεντολών του Word https://support.microsoft.com/el-gr/help/211607/frequently-asked-questions-about-word-macro-viruses
10. Appsealing.com-https://www.appsealing.com/types-of-cyber-attacks/
11. SQL Injection: Μία ασύμμετρη διαδικτυακή απειλή https://www.itsecuritypro.gr/sql-injection-mia-asymmetri-diadiktyaki-apili/
12. What is a UDP Flood | DDoS Attack Glossary | Imperva https://www.imperva.com/learn/ddos/udp-flood/
13. What is a Smurf Attack? | Kaspersky https://www.kaspersky.com/resource-center/definitions/what-is-a-smurf-attack
14. What is Ping of Death (PoD) | DDoS Attack Glossary | Imperva https://www.imperva.com/learn/ddos/ping-of-death/

15. Οι 3 πιο διαδεδομένες απειλές κακόβουλου λογισμικού | Insider https://www.insider.gr/epiheiriseis/tehnologia/109108/oi-3-pio-diadedomenes-apeiles-kakoboyloy-logismikoy

16. What is a Botnet Attack – Definition | Akamai https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp

17. What is address resolution protocol (ARP) and how does it work? Definition from WhatIs.com. https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

18. Zero Day Attacks: Χαρακτηριστικά και Αντιμετώπιση | IT SECURITY PRO: Περιοδικό για το Business IT και την ασφάλεια πληροφοριών| https://www.itsecuritypro.gr/zero-day-attacks-charaktiristika-ke-antimetopisi/

19. What is a Zero-Day Exploit | Protecting Against 0day Vulnerabilities | Imperva https://www.imperva.com/learn/application-security/zero-day-exploit/

20. About Robert Tappan Morris: American computer scientist; creator of Morris Worm; associate professor at MIT (1965-) | Biography, Facts, Career, Wiki, Life https://peoplepill.com/people/robert-tappan-morris/

21. The Morris Worm | Federal Bureau of Investigation https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

22. Top 10 most notorious cyber attacks in history https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

23. MafiaBoy' Michael Calce Discusses the Mindset of a Hacker https://www.insight.com/en_US/content-and-resources/2018/02282018-mafiaboy-michael-calce-discusses-the-mindset-of-a-hacker.html

24. Understanding APIs - Red Hat https://www.redhat.com/en/topics/api

25. What is API security? Definition from WhatIs.com. https://searchapparchitecture.techtarget.com/definition/API-security

26. Peng Peng* , Limin Yang‡ , Linhai Song† , Gang, Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan https://users.cs.fiu.edu/~carbunar/teaching/cis5373/cis5373.S.2020/presentations/virustotal.pdf

27. Rima Masri and Monther Automated Malicious Advertisement Detection using VirusTotal, URLVoid, and TrendMicro https://www.researchgate.net/profile/Monther_Aldwairi/publication/316105179_Automated_Malicious_Advertisement_Detection_using_VirusTotal_URLV

oid_and_TrendMicro/links/59e1cf2a0f7e9b97fbe72ef9/Automated-Malicious-Advertisement-Detection-using-VirusTotal-URLVoid-and-TrendMicro.pdf

28. VirusTotal API version 3 Overview https://developers.virustotal.com/v3.0/reference

29. Frequently Asked Questions – AbuseIPDB https://www.abuseipdb.com/faq.html

30. Fei Peng, Zhui Deng, Xiangyu Zhang, and Dongyan Xu, Purdue University; Zhiqiang Lin, The University of Texas at Dallas; Zhendong Su, University of California, Davis, X-Force: Force-Executing Binary Programs for Security Applications

31. IBM X-Force Exchange https://exchange.xforce.ibmcloud.com/faq#xforce_support

32. Kivy: Cross-platform Python Framework for NUI Developmenthttps://kivy.org/#home

33. What Is a URL? - University of Pennsylvania https://www.cis.upenn.edu/~bcpierce/courses/629/papers/Java-tutorial/networking/urls/definition.html

34. Modern DDoS Protection Techniques: An Overview/ https://www.apriorit.com/dev-blog/559-ddos-protection-techniques

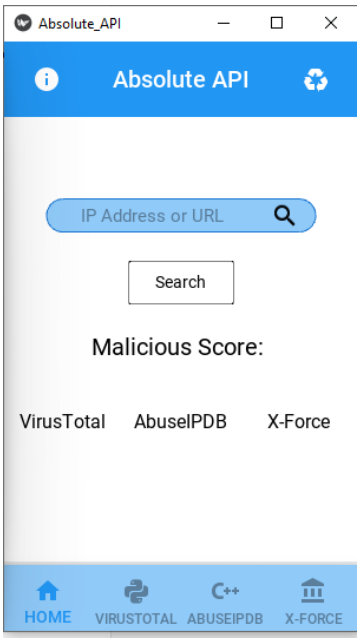
ΠΑΡΑΡΤΗΜΑ

Παραδείγματα εφαρμογής

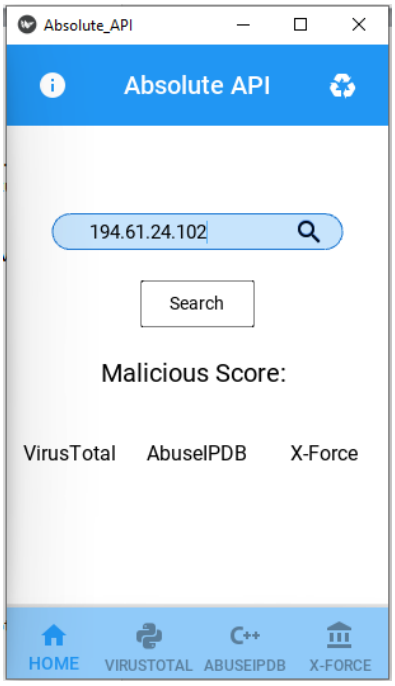
Παράδειγμα 1

Διερεύνηση Ip 194.61.24.102

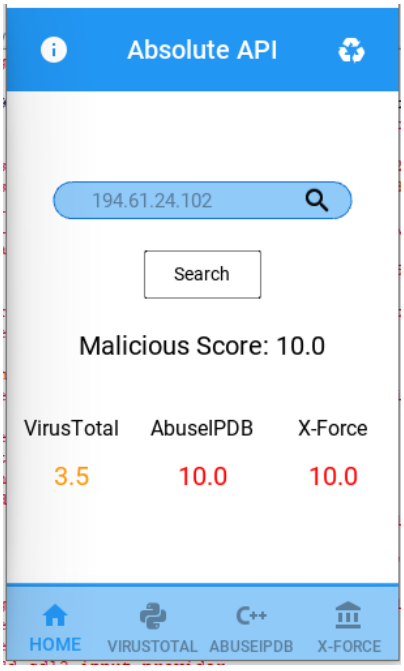
Με την είσοδο στην εφαρμογή, μεταφερόμαστε στην αρχική οθόνη. Το κεντρικό μενού της εφαρμογής έχει την μορφή που φαίνεται παρακάτω.



Εδώ ο χρήστης μπορεί να εκτελέσει βασικές λειτουργίες που προσφέρει η εφαρμογή. Κάνοντας κλικ στο πεδίο αναζήτησης με το φακό δίνεται η δυνατότητα στον χρήστη να καταχωρήσει στο πεδίο text την IP/URL προς αναζήτηση. Για το σκοπό της εργασίας επιλέχθηκε να γίνει αναζήτηση κακόβουλου λογισμικού για την Ip διεύθυνση 194.61.24.102 όπως φαίνεται και στην παρακάτω εικόνα.



Πατώντας ο χρήστης το πλήκτρο search πραγματοποιούνται requests στα 3 API (Virus Total, AbuseIPDB, X-Force). Με την ολοκλήρωση της αναζήτησης, εμφανίζονται τα αντίστοιχα αποτελέσματα χωριστά για κάθε API, καθώς και το τελικό αποτέλεσμα (Malicious Score). Από τα επιμέρους αποτελέσματα, σύμφωνα με τις προδιαγραφές που έχουμε θέσει, το μεγαλύτερο score από τα αποτελέσματα του κάθε API είναι και το τελικό επιθυμητό score το οποίο εμφανίζεται σε ξεχωριστό πεδίο.



Σύμφωνα με τα αποτελέσματα διαπιστώνουμε ότι η IP 194.61.24.102 για τα AbuseIPDB και X-Force API χαρακτηρίζεται ως “Very High Alert IP” με score

10 ενώ αντίθετα για το Virus Total χαρακτηρίζεται ως “Medium Alert” με score 3.5. Το τελικό μας score αντιστοιχεί στο malicious score και είναι 10.
Ο χρήστης επιλέγοντας ένα από τα κουμπιά στο κάτω μέρος του menu έχει την δυνατότητα να αποκτήσει πρόσβαση στα responses για κάθε API ξεχωριστά όπου μπορεί να διατηρήσει ή να επεξεργαστεί την απορρέουσα πληροφορία.

Virus total API response

Σύμφωνα με το αποτέλεσμα του virus total API διαπιστώνουμε ότι κατά την ανάλυση της IP **94.61.24.102** 71 μηχανές χαρακτήρισαν την Ip ως harmless, 3 ως malicious και 1 ως suspicious ενώ 10 από τις μηχανές αναζήτησης δεν έφεραν αποτελέσματα. Το τελικό Score βάση της συνθήκης που έχουμε ορίσει είναι **finalRisk =(malicious * 10) + (suspicious * 5) /10,** και στο παράδειγμα μας το τελικό ρίσκο είναι 3,5 **finalRisk=35/10=3.5**

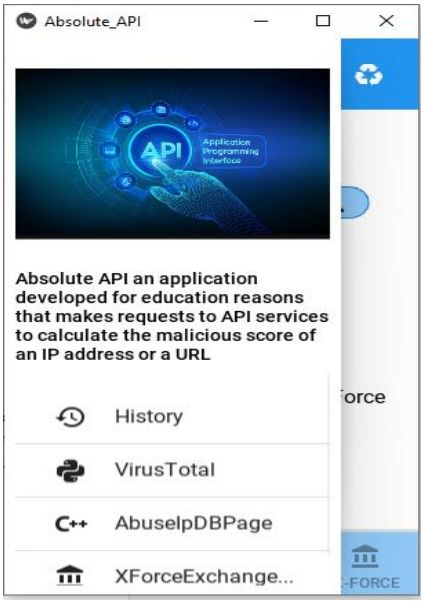
AbuseIPDB response

Σύμφωνα με το αποτέλεσμα του AbuseIpdb API διαπιστώνουμε ότι κατά την ανάλυση της IP 94.61.24.102 το Abuse confidence score είναι 100 και ενώ η Ip έχει γίνει 427 report .

Xforce response

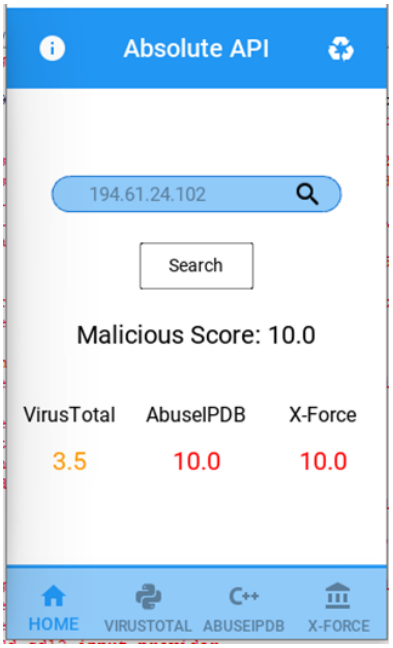
Σύμφωνα με το αποτέλεσμα του Xforce API βλέπουμε ξεχωριστά τα αποτελέσματα των μηχανισμών που χρησιμοποιεί για την ανάλυση της IP

94.61.24.102**.** Επιλέγοντας το button info  στην αριστερή πλευρά του παραθύρου υπάρχει ένα menu-bar, όπου απεικονίζονται 4 κουμπιά:

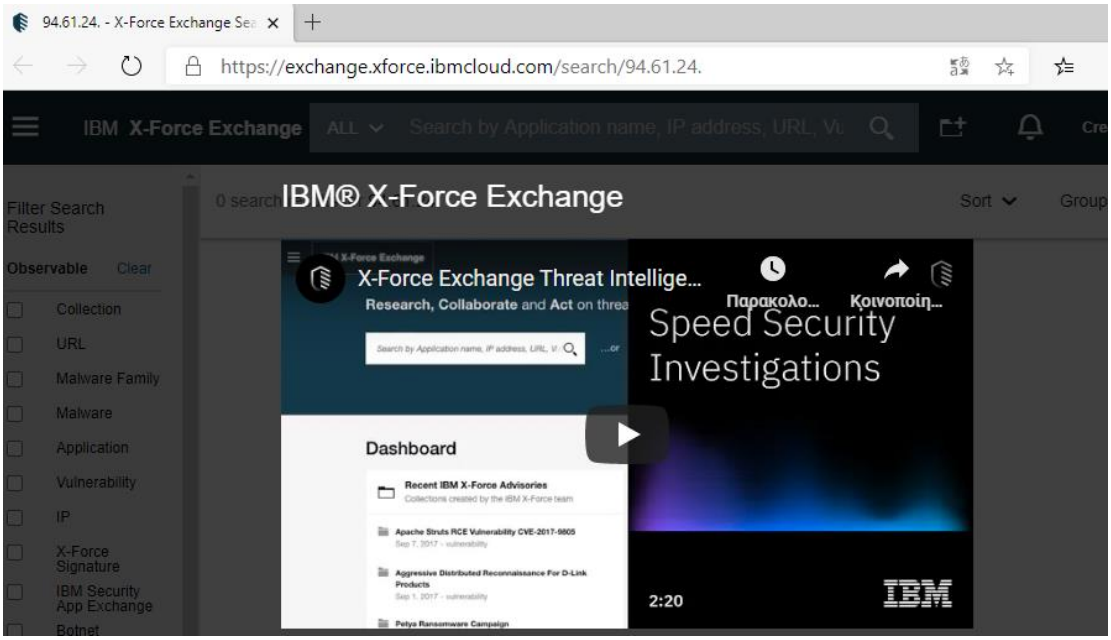


Ο χρήστης επιλέγοντας το history button, έχει την δυνατότητα να αναζητήσει πληροφορίες σχετικά με τα αποτελέσματα των προηγούμενων αναζητήσεων. Με τις υπόλοιπες τρείς επιλογές δίνεται η δυνατότητα στο χρήστη να λάβει πληροφορίες αναφορικά με τις τρεις δημοφιλέστερες μηχανές αναζήτησης κακόβουλου λογισμικού.

Με την επιλογή του button  ο χρήστης έχει την δυνατότητα να μεταβεί στο κεντρικό παράθυρο.



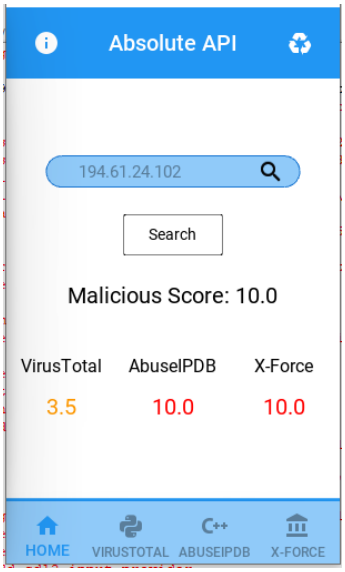
Ο χρήστης κάνοντας κλικ πάνω σε κάποιο από τα επι μέρους αποτελέσματα αυτόματα οδηγείται στην αντίστοιχη ηλεκτρονική διεύθυνση της μηχανής αναζήτησης.



Τέλος με την επιλογή του Button  δίνεται στον χρήστη η δυνατότητα διαγραφής όλων των δεδομένων της τελευταίας αναζήτησης και μετάβασης στο αρχικό παράθυρο της εφαρμογής.

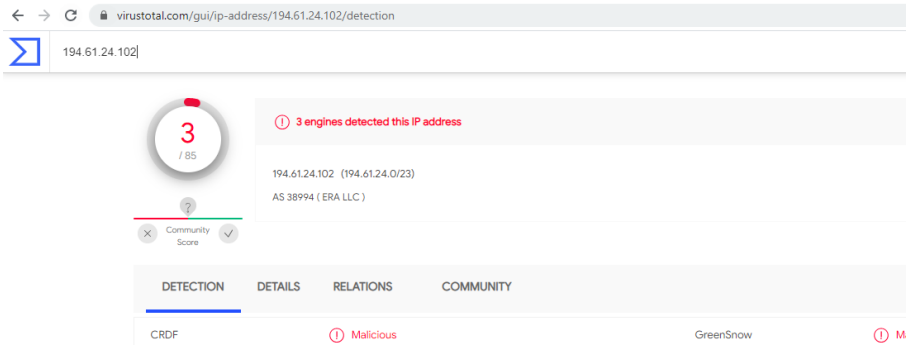
Αποτελέσματα μηχανών αναζήτησης και σύγκριση με τα αποτελέσματα της εφαρμογής

Όπως αναφέραμε παραπάνω, το αποτελέσματα αναζήτησης για την Ip **94.61.24.102** στην εφαρμογή, είναι τα εξής:



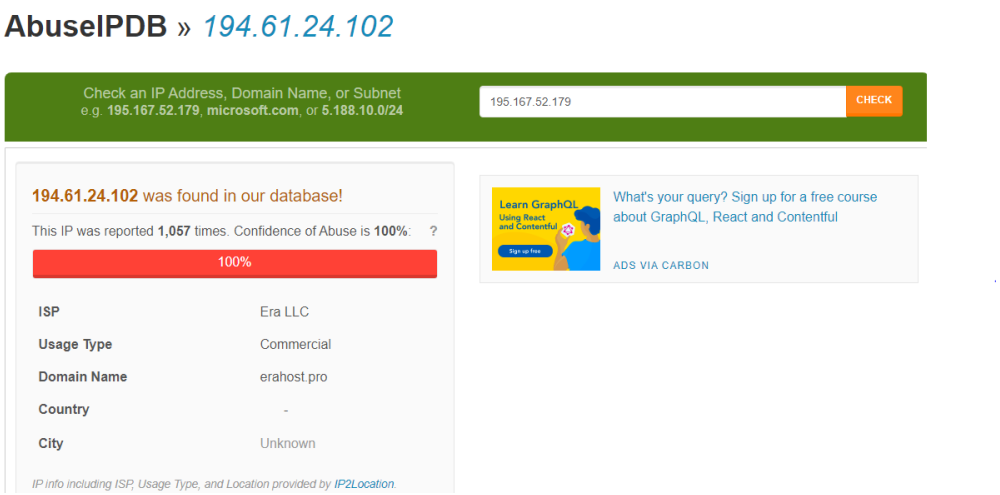
Αποτελέσματα αναζήτησης IP στο Virus Total

Η αναζήτηση της Ip **94.61.24.102** στο Virus total (https://www.virustotal.com) είχε αποτέλεσμα 3 από τις μηχανές αναζήτησης να την ανιχνεύσουν ως κακόβουλη.



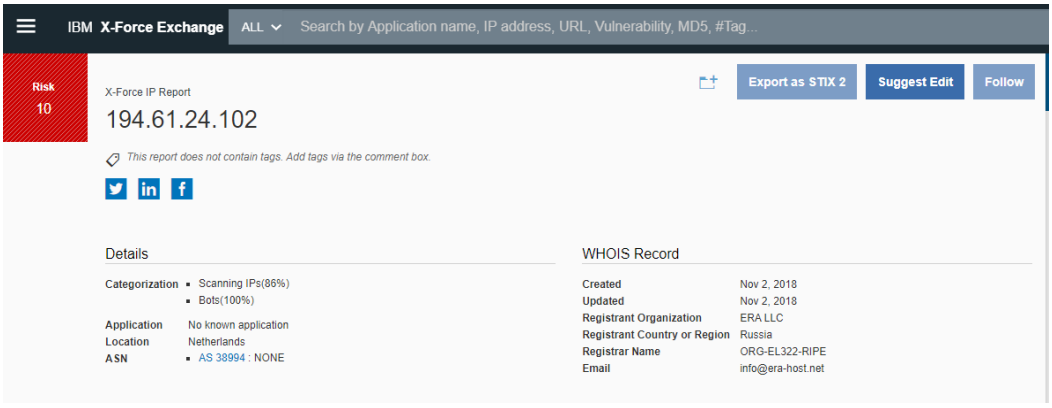
Αποτελέσματα αναζήτησης IP sto AbuseIpdb

Η αναζήτηση της Ip **94.61.24.102** στο AbuseIpdb (https://www.abuseIpdb.com/check) με κλίμακα το 100 χαρακτηρίζεται 100% ως malicious και έχει γίνει report 1057 φορές.



Αποτελέσματα αναζήτησης IP στο X-Force exchange

Η αναζήτηση της της Ip **94.61.24.102** στο X-Force exchange (https://exchange.xforce.ibmcloud.com/) με κλίμακα το 10 χαρακτηρίζεται με ρίσκο 10 ως κακόβουλη.

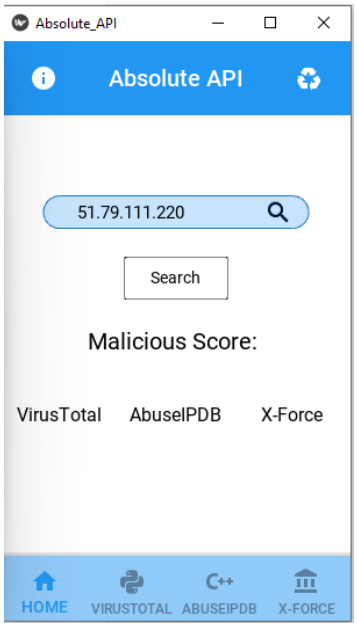


Συμπερασματικά τα αποτελέσματα των τριών Api της εφαρμογής μας αντιστοιχούν με τα αποτελέσματα των τριών μηχανών αναζήτησης.

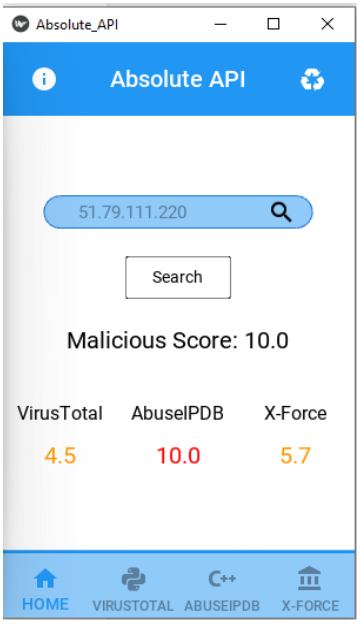
Παράδειγμα 2ο

Διερεύνηση IP 51.79.111.220

Πραγματοποιούμε αναζήτηση της Ip 51.79.111.220 στην εφαρμογή



Σύμφωνα με τα αποτελέσματα που φαίνονται παρακάτω διαπιστώνουμε ότι η Ip 51.79.111.220 για το Virus total και αντίστοιχα για το X-force χαρακτηρίζεται ως Medium Alert με score 4.5. και 5.7 αντίστοιχα ενώ για την AbuseIPDB χαρακτηρίζεται ως very High alert Ip με score 10. Το τελικό μας score αντιστοιχεί στο malicious score και είναι 10.

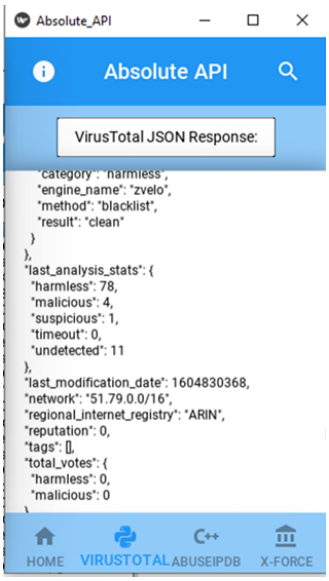


Αποτελέσματα αναζήτησης

API Αποτελέσματα

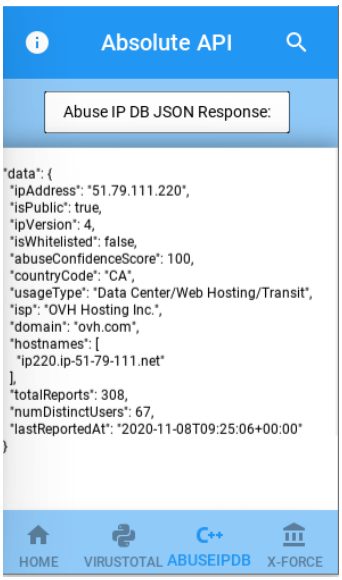
Ο χρήστης, επιλέγοντας ένα από τα κουμπιά στο κάτω μέρος του menu έχει την δυνατότητα να αποκτήσει πρόσβαση στα responses για κάθε API ξεχωριστά όπου μπορεί να διατηρήσει ή να επεξεργαστεί την απορρέουσα πληροφορία. Παρακάτω βλέπουμε ξεχωριστά τα αποτελέσματα των responses για το κάθε API.

Virus total API response



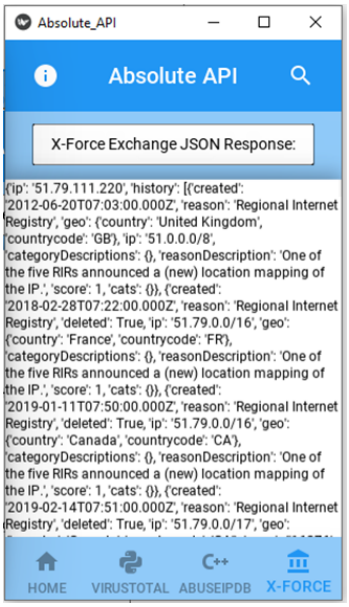
Σύμφωνα με το αποτέλεσμα του virus total API διαπιστώνουμε ότι κατά την ανάλυση της IP **51.79.111.220** 78 μηχανές χαρακτήρισαν την Ip ως harmless 4 ως malicious και 1 ως suspicious ενώ 11 από τις μηχανές αναζήτησης δεν έφεραν αποτελέσματα. Το τελικό Score βάση της συνθήκης που έχουμε ορίσει είναι **finalRisk =(malicious * 10) + (suspicious * 5) /10,** και στο παράδειγμα μας το τελικό ρίσκο είναι 3,5 **finalRisk=45/10=4.5.**

AbuseIPDB API respose



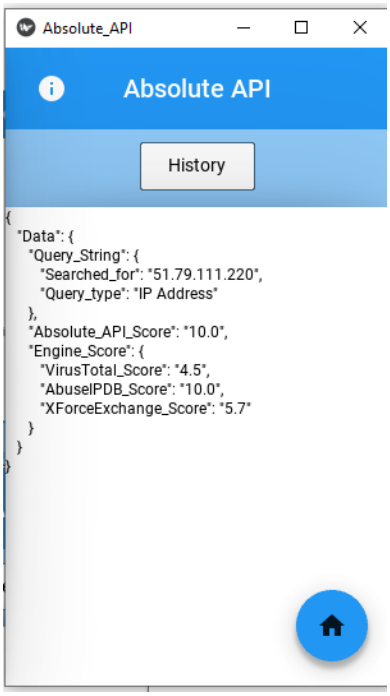
Σύμφωνα με το αποτέλεσμα του AbuseIpdb API διαπιστώνουμε ότι κατά την ανάλυση της IP **51.79.111.220** το Abuseconfidence score είναι 100 και ενώ η Ip έχει γίνει 308 report.

XForce API respose



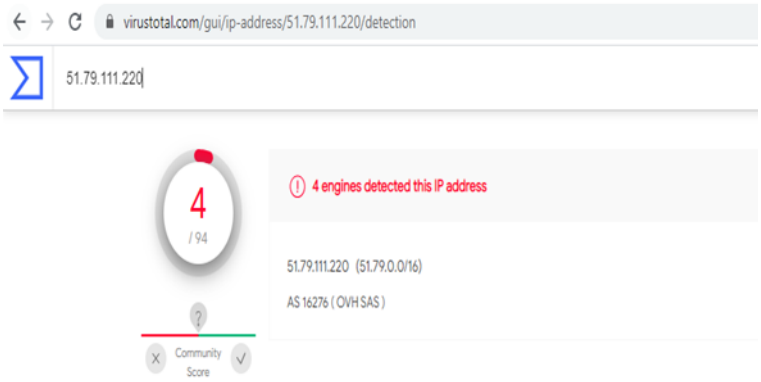
Σύμφωνα με το αποτέλεσμα του Xforce API βλέπουμε ξεχωριστά τα αποτελέσματα των μηχανισμών που χρησιμοποιεί για την ανάλυση της Ip **51.79.111.220.**

Ο χρήστης, επιλέγοντας το history button, έχει την δυνατότητα να αναζητήσει τα αποτελέσματα του τελευταίου Session.

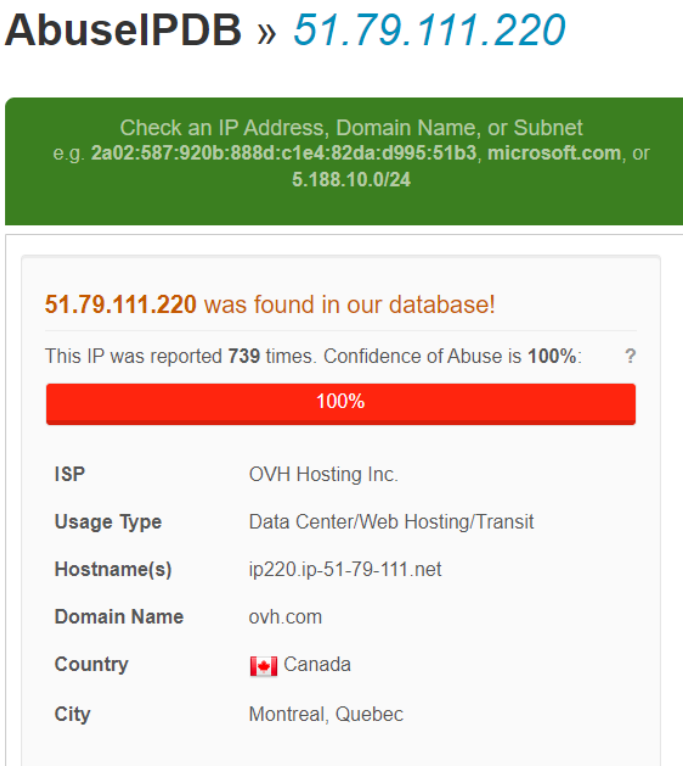


Αποτελέσματα μηχανών αναζήτησης και σύγκριση με τα αποτελέσματα της εφαρμογής

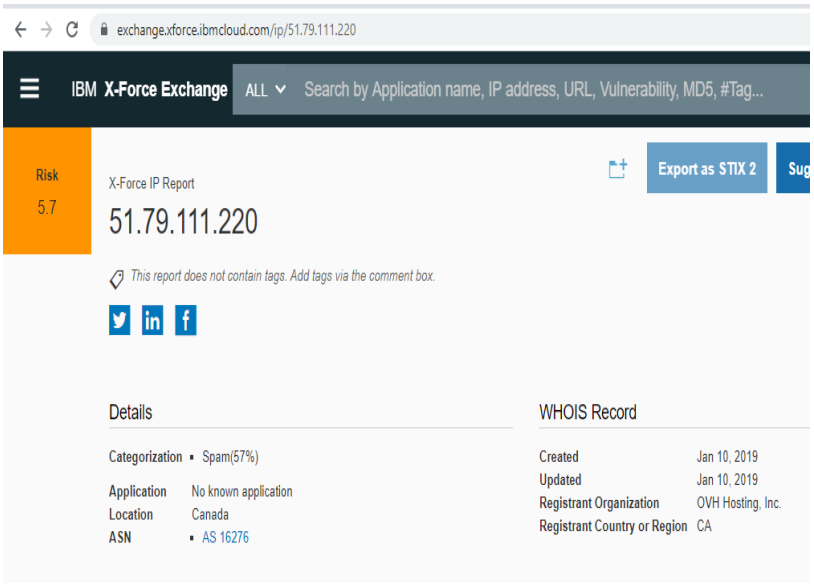
Η αναζήτηση της Ip **51.79.111.220** στο Virus total (https://www.virustotal.com) είχε αποτέλεσμα μόνο 4 από τις μηχανές αναζήτησης να την ανιχνεύσουν ως κακόβουλη.



Η αναζήτηση της Ip στο AbuseIpdb (https://www.abuseIpdb.com/check) με κλίμακα το 100 χαρακτηρίζεται 100% ως malicious. Η συγκεκριμένη Ip **51.79.111.220** έχει γίνει reported 739 φορές.



Τέλος η αναζήτηση της Ip **51.79.111.220** στο X-Force exchange (https://exchange.xforce.ibmcloud.com/)με κλίμακα το 10 χαρακτηρίζεται με ρίσκο 5.7.

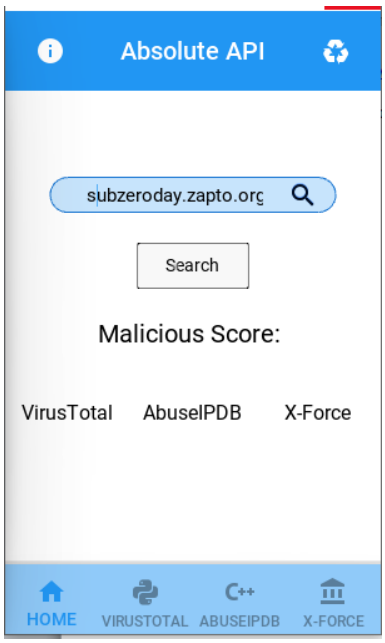


Συμπερασματικά τα αποτελέσματα των τριών Api της εφαρμογής μας αντιστοιχούν με τα αποτελέσματα των τριών μηχανών αναζήτησης.

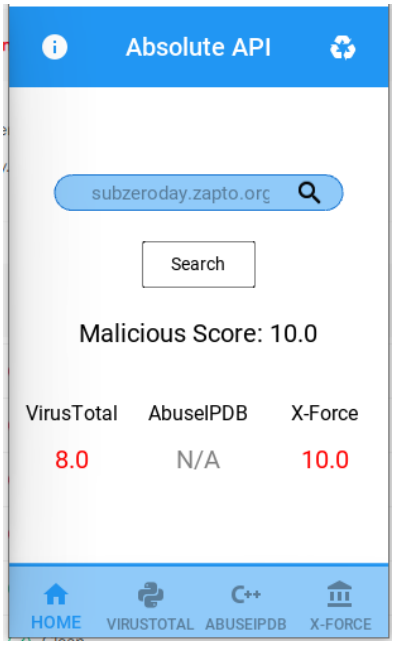
Παράδειγμα 3

Διερεύνηση Url http://subzeroday.zapto.org/

Πραγματοποιούμε αναζήτηση του Url http://subzeroday.zapto.org/ στην εφαρμογή.



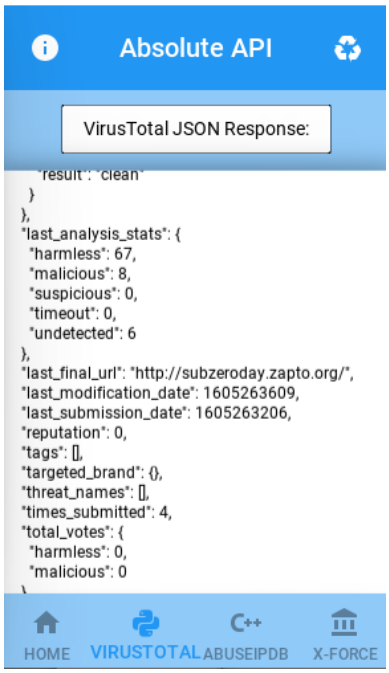
Σύμφωνα με τα αποτελέσματα που προκύπτουν διαπιστώνουμε ότι το Url http://subzeroday.zapto.org/ για το Virus total και αντίστοιχα για το X-force χαρακτηρίζεται ως High Alert με score 8 και 10 αντίστοιχα ενώ για την AbuseIPDB όπως έχουμε ήδη αναφέρει δεν υπάρχει δυνατότητα αναζήτησης Url συνεπώς η απάντηση είναι N/A. Το τελικό μας score αντιστοιχεί στο malicious score και είναι 10.



API Αποτελέσματα

Παρακάτω βλέπουμε ξεχωριστά τα αποτελέσματα των responses για το κάθε API.

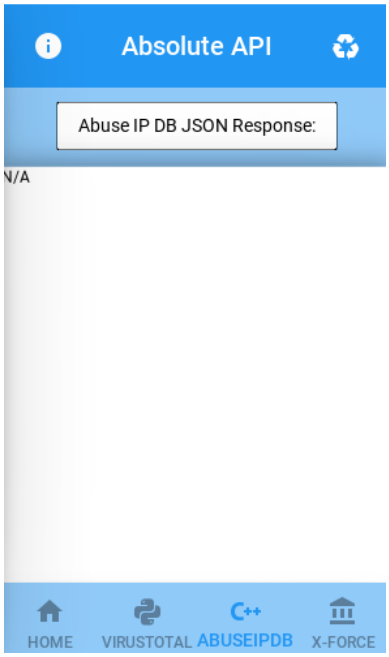
Virus total API response



Σύμφωνα με το αποτέλεσμα του virus total API διαπιστώνουμε ότι κατά την ανάλυση του Url **http://subzeroday.zapto.org** 67 μηχανές χαρακτήρισαν την Ip ως harmless 8 ως malicious και καμία ως suspicious ενώ 6 από τις μηχανές

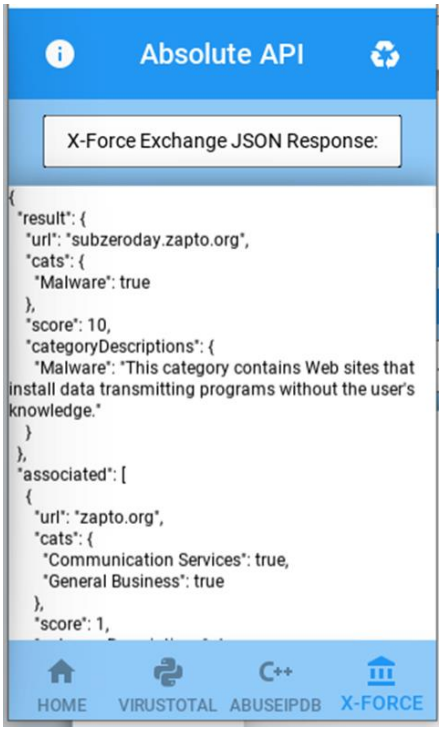
αναζήτησης δεν έφεραν αποτελέσματα. Το τελικό Score βάση της συνθήκης που έχουμε ορίσει είναι **finalRisk =(malicious * 10) + (suspicious * 5) /10,** και στο παράδειγμα μας το τελικό ρίσκο είναι 8 **finalRisk=80/10=8**

AbuseIPDB API response



Σύμφωνα με το αποτέλεσμα του AbuseIpdb API διαπιστώνουμε το αποτέλεσμα είναι Not Available καθώς στο AbuseIpdb δεν μπορεί να γίνει αναζήτηση Url.

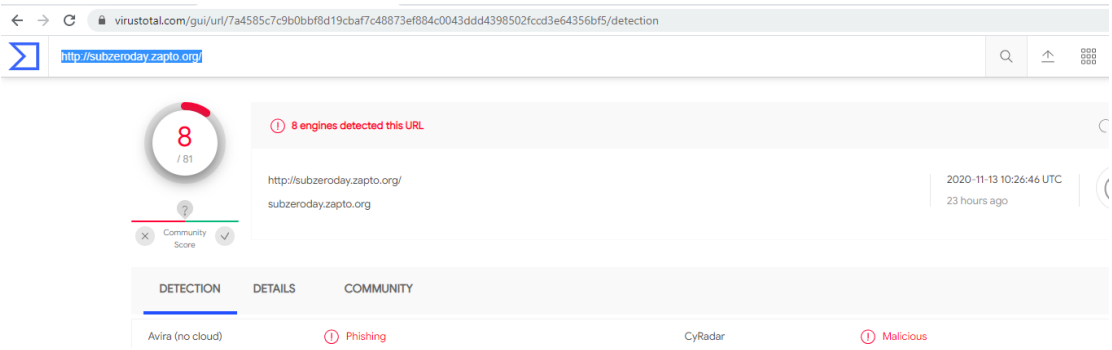
X-Force API response



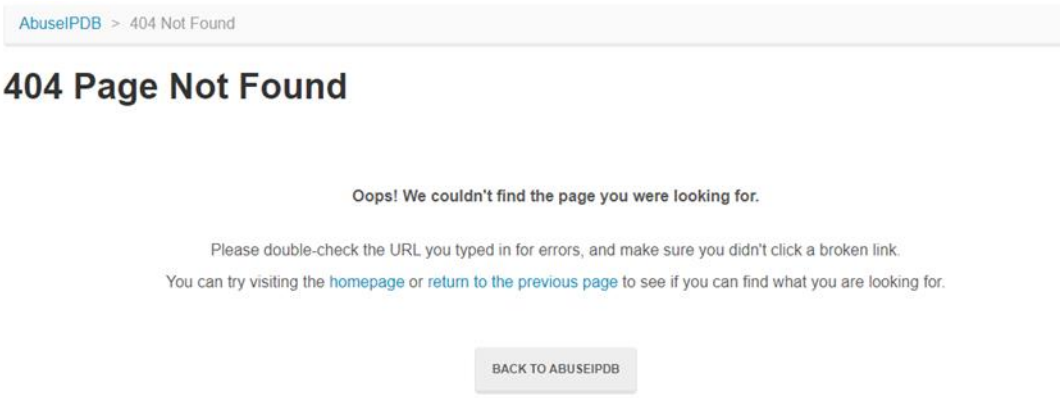
Τέλος η αναζήτηση του Url **http://subzeroday.zapto.org** στο X-Force exchange (https://exchange.xforce.ibmcloud.com/) χαρακτηρίζεται με ρίσκο 10.

Αποτελέσματα μηχανών αναζήτησης και σύγκριση με τα αποτελέσματα της εφαρμογής

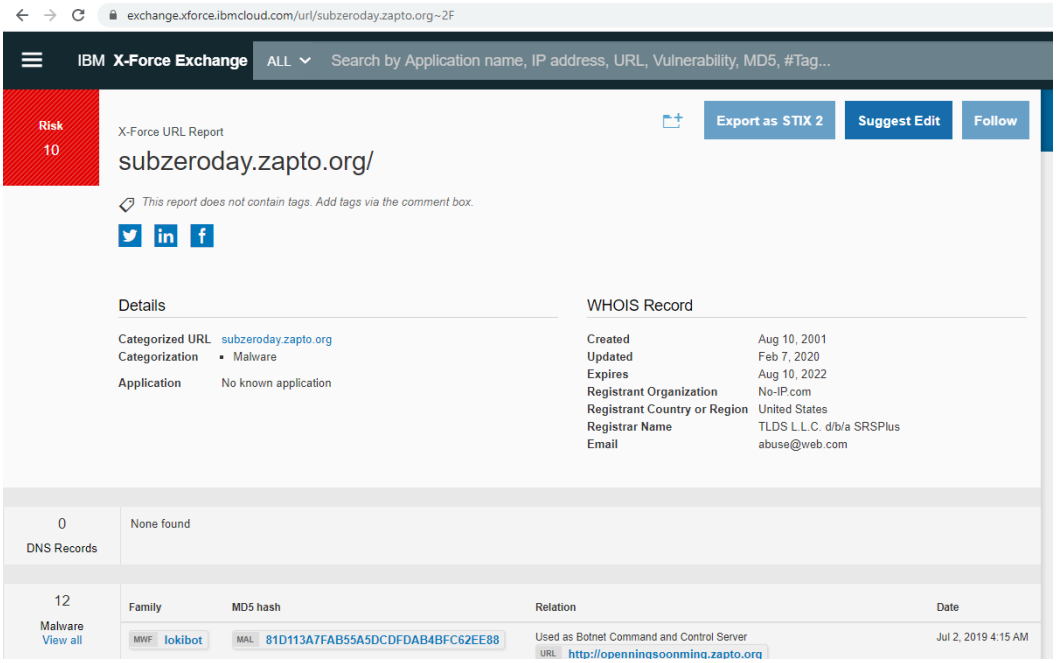
Η αναζήτηση του Url **http://subzeroday.zapto.org** στο Virus total (https://www.virustotal.com) είχε ως αποτέλεσμα 8 από τις μηχανές αναζήτησης να το ανιχνεύσουν ως κακόβουλο.



Η αναζήτηση του Url **http://subzeroday.zapto.org** στο AbuseIpdb δεν επέστρεψε αποτελέσματα.



Τέλος η αναζήτηση του Url **http://subzeroday.zapto.org** στο X-Force exchange (https://exchange.xforce.ibmcloud.com/) με κλίμακα το 10 χαρακτηρίστηκε με ρίσκο 10.

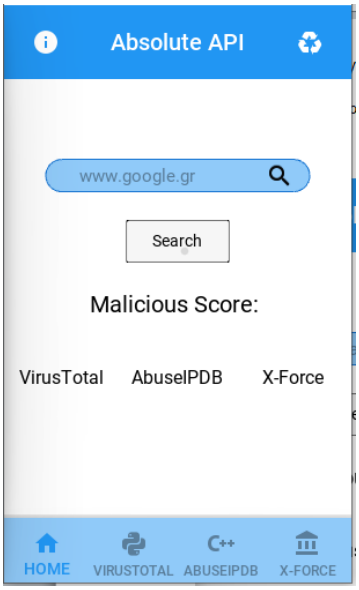


Συμπερασματικά τα αποτελέσματα των τριών Apiτης εφαρμογής μας αντιστοιχούν με τα αποτελέσματα των τριών μηχανών αναζήτησης.

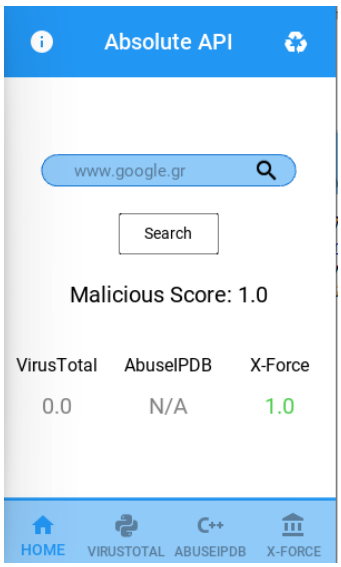
Παράδειγμα 4

Διερεύνηση Url http://www.google.gr

Πραγματοποιούμε αναζήτηση του Url http://www.google.gr στην εφαρμογή



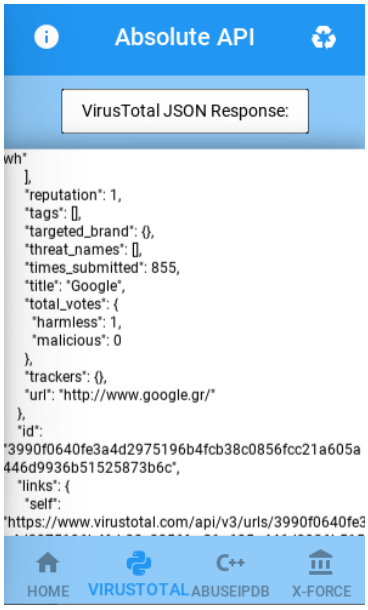
Σύμφωνα με τα αποτελέσματα που προκύπτουν διαπιστώνουμε ότι το Url http://www.google.gr για το Virus total και αντίστοιχα για το X-force χαρακτηρίζεται ώς Low με score 0 και 1 αντίστοιχα ενώ για την AbuseIPDB όπως έχουμε ήδη αναφέρει δεν υπάρχει δυνατότητα αναζήτησης Url συνεπώς η απάντηση είναι N/A(Not available). Το τελικό μας score αντιστοιχεί στο malicious score και είναι 1.



API Αποτελέσματα

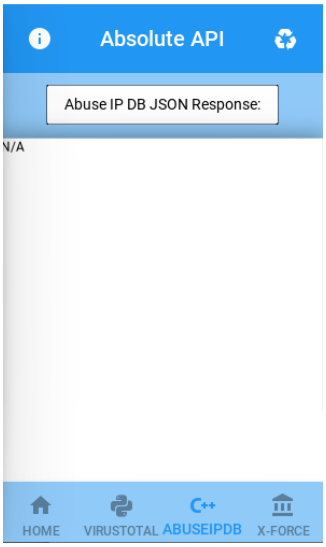
Παρακάτω βλέπουμε ξεχωριστά τα αποτελέσματα των responses για το κάθε API.

Virus total API response



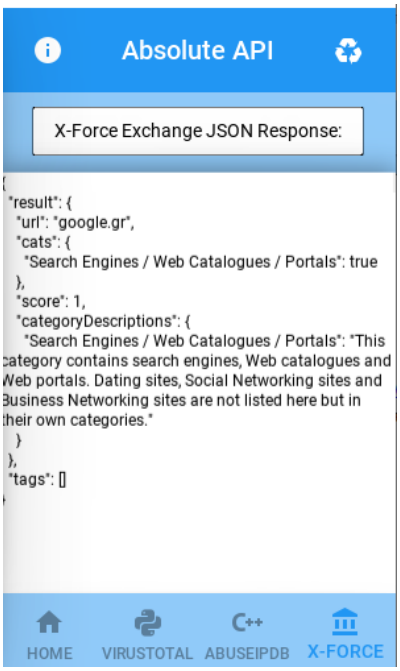
Σύμφωνα με το αποτέλεσμα του virus total API διαπιστώνουμε ότι κατά την ανάλυση του Url **http://www.google.gr** 1 μηχανές χαρακτήρισαν την Ip ως harmless 0 ως malicious και καμία ως suspicious. Το τελικό Score βάση της συνθήκης που έχουμε ορίσει είναι **finalRisk =(malicious * 10) + (suspicious * 5) /10,** και στο παράδειγμα μας το τελικό ρίσκο είναι 1 **finalRisk=0/10=0**

AbuseIPDB API response



Σύμφωνα με το αποτέλεσμα του AbuseIpdb API διαπιστώνουμε το αποτέλεσμα είναι Not Available καθώς στο AbuseIpdb δεν μπορεί να γίνει αναζήτηση Url

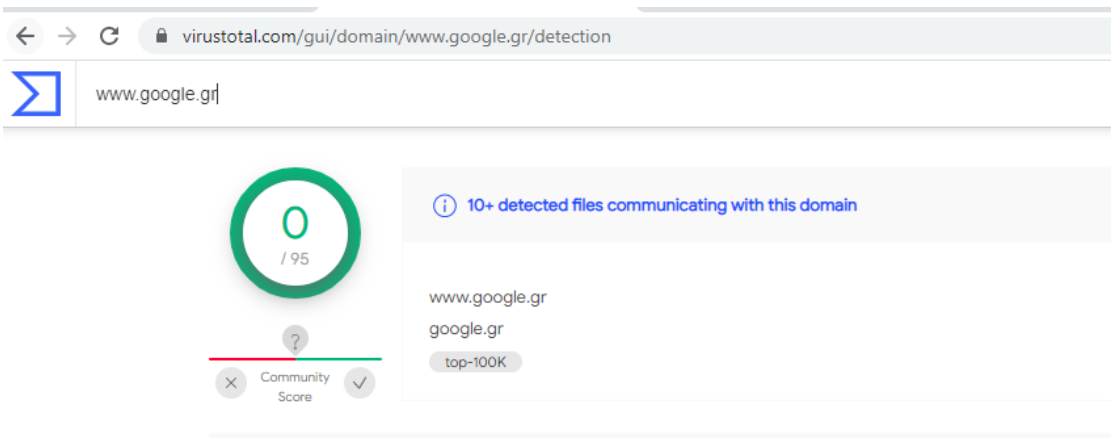
X-FORCE API response



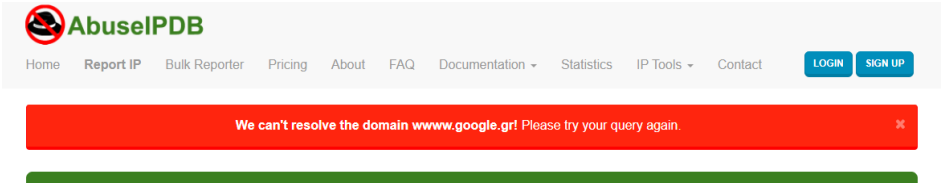
Τέλος η αναζήτηση του Url **www.google.gr** στο X-Force exchange (https://exchange.xforce.ibmcloud.com/) χαρακτηρίζεται με ρίσκο 1.

Αποτελέσματα μηχανών αναζήτησης και σύγκριση με τα αποτελέσματα της εφαρμογής

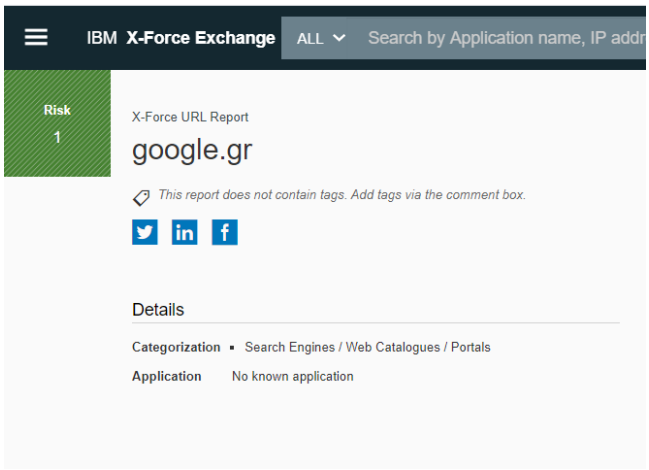
Η αναζήτηση του Url στο virus total είχε αποτέλεσμα καμία από τις μηχανές αναζήτησης να μην το ανιχνεύσει ως κακόβουλο.



Η αναζήτηση του Url www.google.gr στο AbuseIPDB δεν επέστρεψε αποτελέσματα.



Τέλος η αναζήτηση του Url στο X-Force exchange (https://exchange.xforce.ibmcloud.com/) με κλίμακα το 0 χαρακτηρίζεται ως Low risk με αποτέλεσμα 1.

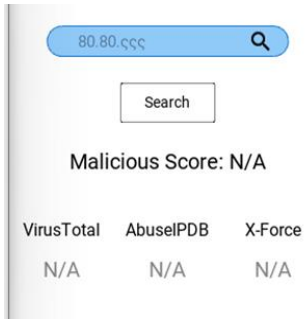


Συμπερασματικά τα αποτελέσματα των τριών API της εφαρμογής μας αντιστοιχούν με τα αποτελέσματα των τριών μηχανών αναζήτησης.

Παράδειγμα 5

Διερεύνηση Λάθους καταχώρησης στο πεδίο αναζήτησης

Στο παράδειγμα μας καταχωρούμε στο πεδίο αναζήτησης την παρακάτω εγγραφή 80.80.ςςς, σύμφωνα με το παράδειγμα μας σε περίπτωση που χρήστης επιλέξει λάθος καταχώρηση τότε αυτόματα θα λάβει απάντηση με αρνητικό αποτέλεσμα.



Κώδικας Εφαρμογής

```
from kivymd.app import MDApp
from kivymd.uix.label import MDLabel, MDIcon
from kivymd.uix.button import MDFlatButton,
MDRectangleFlatButton, MDIconButton, MDFloatingActionButton
from kivymd.uix.textfield import MDTextField, MDTextFieldRect
from kivy.lang import Builder
from kivy.core.window import Window
from kivy.uix.screenmanager import Screen, ScreenManager
from kivy.uix.boxlayout import BoxLayout
from kivymd.uix.list import MDList
from kivymd.theming import ThemableBehavior
from kivy.uix.scrollview import ScrollView
from kivy.uix.widget import Widget
from requests.auth import HTTPBasicAuth
import ipaddress
import requests
import base64
import json

import webbrowser
"""Determine the size of the window (usually 300x500 for
phones)"""
Window.size = (300, 500)

"""The following "screen_helper" is the KV that determines how
objects will be placed and arranged in the app"""
screen_helper = """

WindowManager:
  MainWindow:
  SecondWindow:
  ThirdWindow:
  FourthWindow:
  FifthWindow:


<MainWindow>:
  name: "homePage"

  BoxLayout:
    orientation: 'vertical'
    MDToolbar:
      id: toolbar
      title:'Absolute API'
      anchor_title: 'center'
      left_action_items:     [["information",     lambda     x:
nav_drawer.set_state("open")]]
      right_action_items:      [["recycle",      lambda      x:
root.new_Search(entry,VirusTotal_JSON,          AbuseIPDB_JSON,
```

```
X_FORCE_EXCHANGE_JSON,    VirusTotal_Score,    AbuseIPDB_Score,
X_Force_Exchange_Score, Home, FinalScore, ProgressBar)]]
      elevation : 0
      specific_text_color: 1,1,1,1
    MDBottomNavigation:
      id: mdbnavigation
      md_bg_color: 1, 1, 1, 1
      panel_color: app.theme_cls.primary_light

      MDBottomNavigationItem:
        id: Home
        md_bg_color: app.theme_cls.primary_color
        md_text_color_normal: 1,1,1,1
        name: 'screen 1'
        text: 'Home'
        icon: 'home'

        MDFloatLayout:
          md_bg_color: 1, 1, 1, 1
          MDTextFieldRound:
            id: entry
            text: ""
            hint_text: 'IP Address or URL'
            pos_hint:{'center_x':0.5, 'center_y':0.78}
            size_hint_x:None
            width:200
            height:10
            icon_right: "magnify"
            icon_right_color: app.theme_cls.primary_light
            normal_color: app.theme_cls.primary_light
            color_active: app.theme_cls.primary_light
            md_bg_color: 1, 1, 1, 1


          MDIconButton:
            icon: "magnify"
            pos_hint:{'center_y':0.78}
            pos: (toolbar.width/2 + entry.width /2 - dp(36),0)

            on_press: root.manual_Search(entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,   X_Force_Exchange_Score,   Home,   FinalScore,
ProgressBar)

on_release:root.generate_Risk(entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,       X_Force_Exchange_Score,       FinalScore,
ProgressBar)


          MDRectangleFlatButton:
            text: "Search"
            pos_hint: {"center_x": 0.5, "center_y": 0.63}
```

```
            text_color: 0, 0, 0, 1
            md_bg_color: 1, 1, 1, 1
            elevation: 0
            borders: 2, 'solid', (1,1,1,1.)

            on_press: root.manual_Search(entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,   X_Force_Exchange_Score,   Home,   FinalScore,
ProgressBar)

on_release:root.generate_Risk(entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,       X_Force_Exchange_Score,       FinalScore,
ProgressBar)
          GridLayout:
            orientation: 'vertical'
            cols: 1
            spacing: 10

            Widget:
            Widget:
            Widget:
            Widget:
            Widget:

            MDLabel:
              id:FinalScore
              text: "Malicious Score: "
              font_size: 20
              size_hint_y: 2
              size_hint_x: 1.5
              height: self.texture_size[1]
              text_size: self.size
              halign: 'center'
              valign: 'top'
            GridLayout:
              cols:3
              MDCard:
                elevation: 0
                MDLabel:
                 id: VirusTotal_text
                  text: 'VirusTotal'
                  halign: "center"
                  elevation: 0

              MDCard:
                elevation: 0
                MDLabel:
                  text: "AbuseIPDB"
                  halign: "center"
                  elevation: 0
              MDCard:
                elevation: 0
```

```
      MDLabel:
        text: "X-Force"
        halign: "center"
        elevation: 0

  GridLayout:
    cols:3
    MDCard:
      elevation: 0

      MDLabel:
        color: (1,1,1,1)
        text: ''
        halign: "center"
        elevation: 0
        font_size: 20


    MDCard:
      elevation: 0
      MDLabel:
        text: ""
        color: (1,1,1,1)
        halign: "center"
        elevation: 0
        font_size: 20


    MDCard:
      elevation: 0
      MDLabel:
        text: ""
        color: (1,1,1,1)
        halign: "center"
        elevation: 0
        font_size: 20
    MDFloatLayout:
      MDFlatButton:
        id: VirusTotal_Score
        text: ''
        size_hint_y: 2.2
        size_hint_x: 0.4
        pos_hint: {"center_x": 0.5, "center_y": 0.9}
        on_press: root.hyperlink(tx="VirusTotal")
        md_bg_color:1, 1, 1, 1
        halign: "center"
        elevation: 0
        font_size: 20

      MDFlatButton:
        id: AbuseIPDB_Score
        text: ''
        size_hint_y: 2.2
```

```
                    size_hint_x: 0.4
                    pos_hint: {"center_x": 1.5, "center_y": 0.9}
                    on_press:
root.hyperlink(tx="AbuseIPDB_Score")
                    md_bg_color:1, 1, 1, 1
                    halign: "center"
                    elevation: 0
                    font_size: 20
                  MDFlatButton:
                    id: X_Force_Exchange_Score
                    text: ''
                    size_hint_y: 2.2
                    size_hint_x: 0.4
                    pos_hint: {"center_x": 2.5, "center_y": 0.9}
                    on_press:
root.hyperlink(tx="X_Force_Exchange_Score" )
                    md_bg_color:1, 1, 1, 1
                    halign: "center"
                    elevation: 0
                    font_size: 20

             GridLayout:
                rows:
                Widget:


              FloatLayout:
                MDProgressBar:
                  id: ProgressBar
                  pos_hint:{"center_x":.5, "center_y":.1}
                  value:0
                  type: "intermediate"
      MDBottomNavigationItem:
        name: 'screen 2'
        text: 'VirusTotal'
        icon: 'language-python'
        #on_release: root.manager.current = "VirusTotalPage"
        MDFloatLayout:
          md_bg_color: app.theme_cls.primary_light
          MDRectangleFlatButton:
            text: "VirusTotal JSON Response:"
            on_release: app.root.current = "homePage"
            line_color: 0, 0, 0, 1
            pos_hint: {"center_x": 0.5, "top": 0.97}
            text_color: 0, 0, 0, 1
            md_bg_color: 1, 1, 1, 1
            elevation: 0
            halign:"center"
          MDCard
            pos_hint: {"top": 0.84}
            size: "500dp", "500dp"
            ScrollView:
              MDLabel:
```

```
                text: ""
                id: VirusTotal_JSON
                font_size: 12
                size_hint_y: 35
                size_hint_x: 1
                #text_size:self.width,None
                height: self.texture_size[1]
                valign: 'top'
                text_size: self.size
      MDBottomNavigationItem:
        name: 'screen 3'
        text: 'AbuseIpDb'
        icon: 'language-cpp'
        #on_release: root.manager.current = "AbuseIpDBPage"
        MDFloatLayout:
          md_bg_color: app.theme_cls.primary_light
          MDRectangleFlatButton:
            text: "Abuse IP DB JSON Response:"
            on_release: app.root.current = "homePage"
            line_color: 0, 0, 0, 1
            pos_hint: {"center_x": 0.5, "top": 0.97}
            text_color: 0, 0, 0, 1
            md_bg_color: 1, 1, 1, 1
            elevation: 0
            halign:"center"

          MDCard
            pos_hint: {"top": 0.84}
            size: "200dp", "180dp"
            ScrollView:
              MDLabel:
                text: ""
                id: AbuseIPDB_JSON
                font_size: 12
                size_hint_y: 1.5
                size_hint_x: 1
                height: self.texture_size[1]
                valign: 'top'
                text_size: self.size


      MDBottomNavigationItem:
        name: 'screen 4'
        text: "X-Force"
        icon: 'bank'
        #on_release:           root.manager.current           =
"XForceExchangePage"
        MDFloatLayout:
          md_bg_color: app.theme_cls.primary_light
          MDRectangleFlatButton:
            text: "X-Force Exchange JSON Response:"
            on_release: app.root.current = "homePage"
            line_color: 0, 0, 0, 1
```

```
            pos_hint: {"center_x": 0.5, "top": 0.97}
            text_color: 0, 0, 0, 1
            md_bg_color: 1, 1, 1, 1
            elevation: 0
            halign:"center"

          MDCard
            pos_hint: {"top": 0.84}
            size: "200dp", "1000dp"
            ScrollView:
              MDLabel:
                text:   ""   #"\\n          ThisThisThisThisThi
\\nsThisThinsnsThisThisTnsThisThisThisThisTThisThisThisTsThisT\
\nhisThisThisis is line 1.\\n This is line 2"*100 #\\n
                id: X_FORCE_EXCHANGE_JSON
                font_size: 12
                size_hint_y: 25
                size_hint_x: 1
                height: self.texture_size[1]
                valign: 'top'
                text_size: self.size
  MDNavigationDrawer:
    id: nav_drawer
    ContentNavigationDrawer:
      BoxLayout:
        orientation: 'vertical'
        padding: "8dp"
        spacing: "8dp"
        Image:
          source: "APIimage.jpg"
          width:100
        MDLabel:
          text: "Absolute API an application developed for
education reasons that makes requests to API services to
calculate the malicious score of an IP address or a URL"
          font_style: "Subtitle2"
          size_hint_y: None
          height: self.texture_size[1]

        ScrollView:
          DrawerList:
            id: md_list

            MDList:
              OneLineIconListItem:
                text: "History"
                on_press:
                  root.manager.current = "History"
                  nav_drawer.set_state("close")
                IconLeftWidget:
                  icon:"history"
              OneLineIconListItem:
                text: "VirusTotal"
```

```
                on_press:
                  root.manager.current = "VirusTotal"
                  nav_drawer.set_state("close")
                IconLeftWidget:
                  icon:'language-python'

              OneLineIconListItem:
                text: "AbuseIpDBPage"
                on_press:
                  root.manager.current = "AbuseIpDBPage"
                  nav_drawer.set_state("close")
                IconLeftWidget:
                  icon:'language-cpp'


              OneLineIconListItem:
                text: "XForceExchangePage"
                on_press:
                  root.manager.current = "XForceExchangePage"
                  nav_drawer.set_state("close")
                IconLeftWidget:
                  icon:'bank'
<SecondWindow>:
  name: "History"
  text: "This is History"

  MDFloatLayout:
    md_bg_color: app.theme_cls.primary_light

    MDToolbar:
      title:'Absolute API'
      anchor_title: 'center'
      left_action_items:     [["information",     lambda     x:
drawer2.set_state("open")]]

      elevation : 0
      specific_text_color: 1,1,1,1
      pos_hint: {"top": 1}
      MDIconButton:
        icon:''
        #on_release: app.root.current = "homePage"
        md_bg_color: app.theme_cls.primary_color
        elevation: 0
        pos_hint: {"top": 0.85}
        text_color: 1,0,0,1


    MDRectangleFlatButton:
      text: "History"
      #on_release: app.root.current = "homePage"
      line_color: 0, 0, 0, 1
      pos_hint: {"center_x": 0.5, "top": 0.85}
      text_color: 0, 0, 0, 1
```

```
      md_bg_color: 1, 1, 1, 1
      halign:"center"

    MDCard
      pos_hint: {"center_x": 0.5, "top": 0.75}
      elevation: 10
      halign:"center"
      ScrollView:
        MDLabel:
          id: History_Label
          text: ""
          font_size: 12
          size_hint_y: 10
          size_hint_x: 1
          #text_size:self.width,None
          height: self.texture_size[1]
          valign: 'top'
          text_size: self.size
          #text_color: 1, 0, 0, 1

    MDFloatingActionButton:
      icon: "home"
      elevation_normal: 10
      pos_hint: {"center_x": 0.85, "top": 0.15}
      md_bg_color: app.theme_cls.primary_color
      on_release: app.root.current = "homePage"

  MDNavigationDrawer:
    id: drawer2
    ContentNavigationDrawer:
      BoxLayout:
        orientation: 'vertical'
        padding: "8dp"
        spacing: "8dp"
        Image:
          source:                                    "APIimage.jpg"
##################################################################
###################################
          width:100
        MDLabel:
          text: "Absolute API an application developed for
education reasons that makes requests to API services to
calculate the malicious score of an IP address or a URL:"
          font_style: "Subtitle2"
          size_hint_y: None
          height: self.texture_size[1]

        ScrollView:
          DrawerList:
            id: md_list

            MDList:
              OneLineIconListItem:
```

```
                text: "History"
                on_press:
                  root.manager.current = "History"
                  drawer2.set_state("close")
                IconLeftWidget:
                  icon:"history"

              OneLineIconListItem:
                text: "VirusTotal"
                on_press:
                  root.manager.current = "VirusTotal"
                  drawer2.set_state("close")

                IconLeftWidget:
                  icon:'language-python'

              OneLineIconListItem:
                text: "AbuseIpDBPage"

                on_press:
                  root.manager.current = "AbuseIpDBPage"
                  drawer2.set_state("close")
                IconLeftWidget:
                  icon:'language-cpp'


              OneLineIconListItem:
                text: "XForceExchangePage"
                on_press:
                  root.manager.current = "XForceExchangePage"
                  drawer2.set_state("close")
                IconLeftWidget:
                  icon:'bank'



<ThirdWindow>:
  name: "VirusTotal"
  text: "This is VirusTotal Screen"

  MDFloatLayout:
    md_bg_color: app.theme_cls.primary_light

    MDToolbar:
      title:'Absolute API'
      anchor_title: 'center'
      left_action_items:     [["information",     lambda     x:
drawer3.set_state("open")]]

      elevation : 0
      specific_text_color: 1,1,1,1
      pos_hint: {"top": 1}
```

```
      MDIconButton:
        icon:''
        #on_release: app.root.current = "homePage"
        md_bg_color: app.theme_cls.primary_color
        elevation: 0
        pos_hint: {"top": 0.85}
        text_color: 1,0,0,1


    MDRectangleFlatButton:
      text: "VirusTotal"
      #on_release: app.root.current = "homePage"
      line_color: 0, 0, 0, 1
      pos_hint: {"center_x": 0.5, "top": 0.85}
      text_color: 0, 0, 0, 1
      md_bg_color: 1, 1, 1, 1
      halign:"center"

    MDCard
      pos_hint: {"center_x": 0.5, "top": 0.75}
      elevation: 10
      halign:"center"
      ScrollView:
        MDLabel:
          text:("  " + "Το VirusTotal είναι ένας ιστότοπος που
δημιουργήθηκε από την ισπανική εταιρεία ασφαλείας Hispasec
Sistemas. Ξεκίνησε τον Ιούνιο του 2004, ενώ εξαγοράστηκε από την
Google Inc τον Σεπτέμβριο του 2012. Η ιδιοκτησία της εταιρείας
άλλαξε τον Ιανουάριο του 2018 σε Chronicle, θυγατρική της
Alphabet Inc. Το VirusTotal είναι ένα δωρεάν εργαλείο το οποίο
ο χρήστης μπορεί να εγκατασταθεί σε επιτραπέζιο υπολογιστή ή να
έχει πρόσβαση σε αυτό μέσω διαδικτύου. Το virus total
χρησιμοποιείτε για την ανάλυση ύποπτων αρχεία, hashes ή
διευθύνσεων URL. Χρησιμοποιεί έναν αριθμό μηχανών προστασίας από
ιούς για τη διευκόλυνση της ανίχνευσης διαφορετικών κακόβουλων
λογισμικών, συμπεριλαμβανομένων ιούς, worms και trojans. Εκτός
από τις Antivirus μηχανές, χρησιμοποιεί σαρωτές ιστότοπων για
την ανάλυση και τον εντοπισμό τυχόν κακόβουλου περιεχόμενου
διαθέσιμο σε διευθύνσεις IP/ URL ή αρχεία. Το VirusTotal
χρησιμοποιεί 58 προϊόντα προστασίας από ιούς, όπως το Kaspersky
Lab, Doctor, AVG Technologies, Cyren, περισσότερες από 62
Website/domain μηχανές σάρωσης και datasets όπως το AutoShun,
CRDF,Sucuri SiteCheck, Quttera και περισσότερα από 18 εργαλεία
και σύνολα δεδομένων όπως ExifTool, Snort και Wireshark.")

          font_size: 12
          size_hint_y: 10
          size_hint_x: 1
          #text_size:self.width,None
          height: self.texture_size[1]
          valign: 'top'
          text_size: self.size
          #text_color: 1, 0, 0, 1
```

```
    MDFloatingActionButton:
      icon: "home"
      elevation_normal: 10
      pos_hint: {"center_x": 0.85, "top": 0.15}
      md_bg_color: app.theme_cls.primary_color
      on_release: app.root.current = "homePage"

  MDNavigationDrawer:
    id: drawer3
    ContentNavigationDrawer:
      BoxLayout:
        orientation: 'vertical'
        padding: "8dp"
        spacing: "8dp"
        Image:
          source:                                          "APIimage.jpg"
#################################################################
###################################
          width:100
        MDLabel:
          text: "Absolute API an application developed for
education reasons that makes requests to API services to
calculate the malicious score of an IP address or a URL"
          font_style: "Subtitle2"
          size_hint_y: None
          height: self.texture_size[1]

        ScrollView:
          DrawerList:
            id: md_list

            MDList:
              OneLineIconListItem:
                text: "History"
                on_press:
                  root.manager.current = "History"
                  drawer3.set_state("close")
                IconLeftWidget:
                  icon:"history"

              OneLineIconListItem:
                text: "VirusTotal"
                on_press:
                  root.manager.current = "VirusTotal"
                  drawer3.set_state("close")

                IconLeftWidget:
                  icon:'language-python'

              OneLineIconListItem:
                text: "AbuseIpDBPage"
                on_press:
```

```
                    root.manager.current = "AbuseIpDBPage"
                    drawer3.set_state("close")
                  IconLeftWidget:
                    icon:'language-cpp'


                OneLineIconListItem:
                  text: "XForceExchangePage"
                  on_press:
                    root.manager.current = "XForceExchangePage"
                    drawer3.set_state("close")

                  IconLeftWidget:
                    icon:'bank'



<FourthWindow>:
  name: "AbuseIpDBPage"
  text: "This is AbuseIpDBPage"
  MDFloatLayout:
    md_bg_color: app.theme_cls.primary_light

    MDToolbar:
      title:'Absolute API'
      anchor_title: 'center'
      left_action_items:     [["information",     lambda     x:
drawer4.set_state("open")]]

      elevation : 0
      specific_text_color: 1,1,1,1
      pos_hint: {"top": 1}
      MDIconButton:
        icon:''
        #on_release: app.root.current = "homePage"
        md_bg_color: app.theme_cls.primary_color
        elevation: 0
        pos_hint: {"top": 0.85}
        text_color: 1,0,0,1


    MDRectangleFlatButton:
      text: "AbuseIpDBPage"
      #on_release: app.root.current = "homePage"
      line_color: 0, 0, 0, 1
      pos_hint: {"center_x": 0.5, "top": 0.85}
      text_color: 0, 0, 0, 1
      md_bg_color: 1, 1, 1, 1
      halign:"center"

    MDCard
      pos_hint: {"center_x": 0.5, "top": 0.75}
```

```
      elevation: 10
      halign:"center"
      ScrollView:
        MDLabel:
          text: "  " + "Το AbuseIPDB αποτελεί μια βάση δεδομένων
αφιερωμένη στο να βοηθά τους διαχειριστές συστημάτων και τους
webmaster να ελέγχουν και να αναφέρουν διευθύνσεις IP που
εμπλέκονται σε κακόβουλη δραστηριότητα, όπως ανεπιθύμητη
αλληλογραφία, απόπειρες εισβολής, επιθέσεις DDoS κ.λπ. Για την
AbuseIPDB, θεωρείτε κακόβουλη κάθε παράνομη, καταχρηστική ή
ακατάλληλη δραστηριότητα που εντοπίστηκε σε μια διεύθυνση IP,
όπως απόπειρα DDoS, κάθε είδους ανεπιθύμητο περιεχόμενο, δόλιες
παραγγελίες, απόπεΙρες εισβολής, phishing, πλαστογράφηση, SQL
injection κα. Το AbuseIPDB μπορεί να λαμβάνει αναφορές για
καθολικές IP μαύρης λίστας. Επειδή αυτή η βάση δεδομένων
περιλαμβάνει παγκόσμιες μαύρες λίστες. Η χρήση της βάσης του
AbuseIPDB είναι δωρεάν για τους χρήστες λόγω περιορισμένων πόρων
συνεπώς η δυνατότητα αναζήτησης είναι περιορισμένη και έγκειται
στα 1.000 αιτήματα / ημέρα τόσο για έλεγχο IP όσο και για
ενέργειες αναφοράς μέσω του δωρεάν API , για webmaster 3.000
αιτήματα / ημέρα. Για τους υποστηριχτές οι οποίοι στηρίζουν
οικονομικά την λειτουργία του AbuseIPDB 5.000 αιτήματα / ημέρα.
"


          font_size: 12
          size_hint_y: 10
          size_hint_x: 1
          #text_size:self.width,None
          height: self.texture_size[1]
          valign: 'top'
          text_size: self.size
          #text_color: 1, 0, 0, 1

    MDFloatingActionButton:
      icon: "home"
      elevation_normal: 10
      pos_hint: {"center_x": 0.85, "top": 0.15}
      md_bg_color: app.theme_cls.primary_color
      on_release: app.root.current = "homePage"

  MDNavigationDrawer:
    id: drawer4
    ContentNavigationDrawer:
      BoxLayout:
        orientation: 'vertical'
        padding: "8dp"
        spacing: "8dp"
        Image:
          source:                                    "APIimage.jpg"
#################################################################
###################################
          width:100
```

```
        MDLabel:
          text: "Absolute API an application developed for
education reasons that makes requests to API services to
calculate the malicious score of an IP address or a URL"
          font_style: "Subtitle2"
          size_hint_y: None
          height: self.texture_size[1]

        ScrollView:
          DrawerList:
            id: md_list

            MDList:
              OneLineIconListItem:
                text: "History"
                on_press:
                  root.manager.current = "History"
                  drawer4.set_state("close")
                IconLeftWidget:
                  icon:"history"

              OneLineIconListItem:
                text: "VirusTotal"
                on_press:
                  root.manager.current = "VirusTotal"
                  drawer4.set_state("close")

                IconLeftWidget:
                  icon:'language-python'

              OneLineIconListItem:
                text: "AbuseIpDBPage"

                on_press:
                  root.manager.current = "AbuseIpDBPage"
                  drawer4.set_state("close")
                IconLeftWidget:
                  icon:'language-cpp'


              OneLineIconListItem:
                text: "XForceExchangePage"
                on_press:
                  root.manager.current = "XForceExchangePage"
                  drawer4.set_state("close")

                IconLeftWidget:
                  icon:'bank'



<FifthWindow>:
```

```
  name: "XForceExchangePage"
  text: "This is XForceExchangePage"
  MDFloatLayout:
    md_bg_color: app.theme_cls.primary_light

    MDToolbar:
      title:'Absolute API'
      anchor_title: 'center'
      left_action_items:     [["information",     lambda     x:
drawer5.set_state("open")]]

      elevation : 0
      specific_text_color: 1,1,1,1
      pos_hint: {"top": 1}
      MDIconButton:
        icon:''
        #on_release: app.root.current = "homePage"
        md_bg_color: app.theme_cls.primary_color
        elevation: 0
        pos_hint: {"top": 0.85}
        text_color: 1,0,0,1


    MDRectangleFlatButton:
      text: "XForceExchangePage"
      #on_release: app.root.current = "homePage"
      line_color: 0, 0, 0, 1
      pos_hint: {"center_x": 0.5, "top": 0.85}
      text_color: 0, 0, 0, 1
      md_bg_color: 1, 1, 1, 1
      halign:"center"

    MDCard
      pos_hint: {"center_x": 0.5, "top": 0.75}
      elevation: 10
      halign:"center"
      ScrollView:
        MDLabel:
          text: "Το IBM® X-Force Exchange είναι μια πλατφόρμα
ανταλλαγής πληροφοριών για απειλές που βασίζεται σε cloud και
μπορεί να χρησιμοποιηθεί για την γρήγορη έρευνα των πιο πρόσφατων
παγκόσμιων απειλών για την ασφάλεια, την συγκέντρωση πληροφοριών
με δυνατότητα δράσης. Το XFE προορίζεται πρωτίστως για αναλυτές
ασφαλείας, αλλά οποιοσδήποτε στον χώρο ασφαλείας μπορεί να λάβει
αξία από το XFE, συμπεριλαμβανομένων μελών ενός κέντρου
επιχειρήσεων ασφαλείας (SOC), φορέων ασφαλείας δικτύου,
διαχειριστών ασφαλείας και επικεφαλής αξιωματικών ασφαλείας
πληροφοριών. Το XFE είναι ένα δωρεάν προϊόν SaaS (Security as a
service) που μπορεί να χρησιμοποιηθεί για να γίνει αναζήτηση της
πληροφορίες σχετικά με απειλές, για την συλλογή ευρημάτων και
τον διαμοιρασμό της πληροφορίας με άλλα μέλη της κοινότητας XFE.
Μπορεί να πραγματοποιηθεί αναζήτηση διευθύνσεων IPv4 και IPv6,
διευθύνσεων URL, ευπάθειες (χρησιμοποιώντας έναν αριθμό CVE),
```

ένα όνομα εφαρμογής, όπως Skype και κατακερματισμούς MD5. Τέλος υπάρχει η δυνατότητα ομαδοποίησης των αποτελεσμάτων αναζήτησης ανά κατηγορία μέσω της επιλογής στοιχείων ομάδας . Οι πληροφορίες που παρέχονται από την X-Force για οποιονδήποτε τύπο αναζήτησης, οι οποίες επιστρέφονται σε μια «αναφορά», προέρχονται από την εσωτερική της υποδομή και βάσεις δεδομένων, καθώς και από περιεχόμενο ανοιχτού κώδικα και συνεργασίες τρίτων μερών για την αύξηση αυτών των πληροφοριών. Το X-Force παρέχει βαθμολογία κινδύνου, τοποθεσία, πληροφορίες κατηγοριοποίησης, ιστορικό περιεχόμενο, πληροφορίες και παθητικές DNS για IP"

```
          font_size: 12
          size_hint_y: 10
          size_hint_x: 1
          #text_size:self.width,None
          height: self.texture_size[1]
          valign: 'top'
          text_size: self.size
          #text_color: 1, 0, 0, 1

    MDFloatingActionButton:
      icon: "home"
      elevation_normal: 10
      pos_hint: {"center_x": 0.85, "top": 0.15}
      md_bg_color: app.theme_cls.primary_color
      on_release: app.root.current = "homePage"

  MDNavigationDrawer:
    id: drawer5
    ContentNavigationDrawer:
      BoxLayout:
        orientation: 'vertical'
        padding: "8dp"
        spacing: "8dp"
        Image:
          source:                                    "APIimage.jpg"
##################################################################
###################################
          width:100
        MDLabel:
          text: "Absolute API an application developed for
education reasons that makes requests to API services to
calculate the malicious score of an IP address or a URL"
          font_style: "Subtitle2"
          size_hint_y: None
          height: self.texture_size[1]

        ScrollView:
          DrawerList:
            id: md_list

            MDList:
              OneLineIconListItem:
                text: "History"
```

```
                on_press:
                  root.manager.current = "History"
                  drawer5.set_state("close")
                IconLeftWidget:
                  icon:"history"

              OneLineIconListItem:
                text: "VirusTotal"
                on_press:
                  root.manager.current = "VirusTotal"
                  drawer5.set_state("close")

                IconLeftWidget:
                  icon:'language-python'

              OneLineIconListItem:
                text: "AbuseIpDBPage"

                on_press:
                  root.manager.current = "AbuseIpDBPage"
                  drawer5.set_state("close")
                IconLeftWidget:
                  icon:'language-cpp'


              OneLineIconListItem:
                text: "XForceExchangePage"
                on_press:
                  root.manager.current = "XForceExchangePage"
                  drawer5.set_state("close")
                IconLeftWidget:
                  icon:'bank'



"""


class MainWindow(Screen):

  """Function to get the entered IP Address and call APIs and
calculate Risk function"""
  def         generate_Risk(self,         entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,       X_Force_Exchange_Score,       FinalScore,
ProgressBar):

    """ When a new search is executed initialize the following
variables: """
    VirusTotal_Score.text = ""
    AbuseIPDB_Score.text= ""
    X_Force_Exchange_Score.text = ""
    VirusTotal_JSON.text= ""
```

```
    AbuseIPDB_JSON.text= ""
    X_FORCE_EXCHANGE_JSON.text= ""
    FinalScore.text="Malicious Score: "

    """Call the valid_ip function"""
    self.valid_ip(entry,VirusTotal_JSON,        AbuseIPDB_JSON,
X_FORCE_EXCHANGE_JSON,    VirusTotal_Score,    AbuseIPDB_Score,
X_Force_Exchange_Score, FinalScore, ProgressBar)
    return


  """Checks if given stirng is IP or Not"""
  def validation(self, entry):
    try:
      (ipaddress.ip_address(entry.text))
      return True
    except:
      """Not an ip"""
      return False


  """If the given string is IP calls the calculate_IP_Risk
function else calls the calculate_URL_Risk function"""
  def  valid_ip(self,  entry,VirusTotal_JSON,  AbuseIPDB_JSON,
X_FORCE_EXCHANGE_JSON,    VirusTotal_Score,    AbuseIPDB_Score,
X_Force_Exchange_Score, FinalScore, ProgressBar):

    if self.validation(entry):
      self.calculate_IP_Risk(entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,       X_Force_Exchange_Score,       FinalScore,
ProgressBar)
    else:
      self.calculate_URL_Risk(entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,       X_Force_Exchange_Score,       FinalScore,
ProgressBar)
    return

  """Function that calls the 3 APIs and then calls the
calculate_final_Risk function (This function will be called if
the user searches for IP Address)"""
  def      calculate_IP_Risk(self,      entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,       X_Force_Exchange_Score,       FinalScore,
ProgressBar):

    """Initialize the following variables"""
    scoreVT = 0
    scoreAB = 0
    scoreX = 0

    """Determine how each of the results will be produced"""
```

```
    VT_Score   =   self.get_VT_Risk_IP(entry,   VirusTotal_JSON,
VirusTotal_Score, scoreVT)
    AbuseIpDB_Score                                          =
self.get_AbuseIpDB_Risk_IP(entry,AbuseIPDB_JSON,
AbuseIPDB_Score, scoreAB)
    XFE_Score           =           self.get_XFE_Risk_IP(entry,
X_FORCE_EXCHANGE_JSON, X_Force_Exchange_Score, scoreX)

    """Calculate the final score"""
    final_score = (max(VT_Score, AbuseIpDB_Score, XFE_Score))
    if      ((VirusTotal_Score.text      ==      "N/A")      and
(AbuseIPDB_Score.text == "N/A") and (X_Force_Exchange_Score.text
== "N/A")):
      final_score = "N/A"
    FinalScore.text = "Malicious Score: " + str(final_score)
    Query_type = 'IP Address'

    """Add search to history"""
    self.Add_To_History(entry,                VirusTotal_Score,
AbuseIPDB_Score,      X_Force_Exchange_Score,      final_score,
Query_type)

    """Visual indication for search completion"""
    ProgressBar.value = 100

    Return


  """Gets Risk for IP Address from VT API"""
  def     get_VT_Risk_IP(self,     entry,     VirusTotal_JSON,
VirusTotal_Score, score):

    """Making request to the API and capturing its response - At
the same the API Key is sent in the header for authentication
resons"""
    response                =                requests.get(url=
'https://www.virustotal.com/api/v3/ip_addresses/' + entry.text,
headers={"x-
apikey":"eb030a8bdb7c29588aec133be486853191b59d9805a9baa4b9dd9d
9099a61eaa"})

    """ If the Api returns a valid response calculate the score
else print "N/A" """
    if response.status_code == 200:

      json_response = response.json()
      data = json_response["data"]

      uglyjson = response.json()
      VirusTotal_JSON.text =(json.dumps(uglyjson, indent=2))

      for key,value in data.items():
```

```
        if key=='attributes':
          attributes=value

      for key,value in attributes.items():

        if key=='last_analysis_stats':
          last_analysis_stats=value

      """The followin part checks the Virustotal Response and
tracks how many engines returned harmless, malicious and
suspicious result"""
      for key,value in last_analysis_stats.items():

        if key =='harmless':
          harmless=value
        if key =='malicious':
          malicious=value
        if key =='suspicious':
          suspicious=value
        if key =='timeout':
          timeout=value
        if key =='undetected':
          undetected=value

      #total = harmless + malicious + suspicious
      """The following formula converts the Virustotal Score to
{0,10} range"""
      finalRisk =(malicious * 10) + (suspicious * 5)

      if finalRisk>100:
        finalRisk = 100

      score = round((finalRisk/10),1)

      self.getScore(VirusTotal_Score, score)

    else:

      VirusTotal_Score.text = "N/A"
      VirusTotal_Score.text_color = (130/255,130/255,130/255,1)

    return score


  """Gets Risk for IP Address from AbuseIpDB API"""
  def     get_AbuseIpDB_Risk_IP(self,entry,     AbuseIPDB_JSON,
AbuseIPDB_Score, score):

    """url and querystring are parameters that will be used in
the API request"""
    url = 'https://api.abuseipdb.com/api/v2/check'
    querystring = {
      'ipAddress': entry.text,
```

```
      'maxAgeInDays': '90'
    }
    headers = {
      'Accept': 'application/json',
      'Key':
'4e4ff2e38b9914bbf76f72aa8e993345c6f7c312246c84ec1ddc9b1d06970d
80ae757e2e3f1b5b81'
    }

    """Making request to the API and capturing its response - At
the same the API Key is sent in the header for authentication
resons"""
    response    =    requests.request(method='GET',    url=url,
headers=headers, params=querystring)

    """ If the Api returns a valid response calculate the score
else print "N/A" """
    if response.status_code == 200:

      json_response = response.json()
      uglyjson = response.json()
      AbuseIPDB_JSON.text =(json.dumps(uglyjson, indent=2))
      Tags = json_response["data"]

      """The following formula converts the Abuse IP DB Score to
{0,10} range"""
      for key, value in Tags.items():

        if "abuseConfidenceScore" in key:
          score = round((value/10),1)

      self.getScore(AbuseIPDB_Score, score)

    else:

      AbuseIPDB_Score.text = "N/A"
      AbuseIPDB_Score.text_color = (130/255,130/255,130/255,1)

    return score

  """Gets Risk for IP Address from xForce API"""
  def   get_XFE_Risk_IP(self,   entry,   X_FORCE_EXCHANGE_JSON,
X_Force_Exchange_Score, score):

    """Making request to the API and capturing its response - At
the same useing basic_authentication to authenticate ourselves
to the API"""
    response                                                =
requests.get('https://api.xforce.ibmcloud.com/ipr/'           +
entry.text,        auth=HTTPBasicAuth('ab51ab4e-90ac-4637-80ad-
4d297981c6d8', 'cd23e237-e38c-4378-9e0c-500c1b316893'))
```

```
    """ If the Api returns a valid response calculate the score
else print "N/A" """
    if response.status_code == 200:

      json_response = response.json()
      X_FORCE_EXCHANGE_JSON.text = str(json_response)

      """The following formula determines the X-FORCE Score"""
      finalScore = json_response['score']
      score = round((finalScore*10)/10,1)

      self.getScore(X_Force_Exchange_Score, score)

    else:

      X_Force_Exchange_Score.text = "N/A"
      X_Force_Exchange_Score.text_color                        =
(130/255,130/255,130/255,1)

    return score

  """Applies color to the inbetween results and asigns the
engines final results that will be displayed in the home
screen"""
  def getScore(self, Engine_Score, score):
    if score > 6.7:
      Engine_Score.text_color = (1,0,0,1)
    elif score > 3.4:
      Engine_Score.text_color = (1,0.6,0,1)
    elif score > 0:
      Engine_Score.text_color = (0.3,0.8,0.3,1)
    elif score == 0:
      Engine_Score.text_color = (130/255,130/255,130/255,1)

    Engine_Score.text = str(score)
    return


  """Calculates Risk for given URL"""
  def      calculate_URL_Risk(self,      entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,       X_Force_Exchange_Score,       FinalScore,
ProgressBar):

    scoreVT = 0
    scoreAB = 0
    scoreX = 0
    """Determine how each of the results will be produced"""
    VT_Score   =   self.get_VT_Risk_URL(entry,   VirusTotal_JSON,
VirusTotal_Score, scoreVT)
    AbuseIpDB_Score     =     self.get_AbuseIpDB_Risk_URL(entry,
AbuseIPDB_JSON, AbuseIPDB_Score, scoreAB)
```

```
    XFE_Score           =           self.get_XFE_Risk_URL(entry,
X_FORCE_EXCHANGE_JSON, X_Force_Exchange_Score, scoreX)


    """Calculate the final score"""
    final_score = (max(VT_Score, XFE_Score))
    if      ((VirusTotal_Score.text      ==      "N/A")      and
(AbuseIPDB_Score.text == "N/A") and (X_Force_Exchange_Score.text
== "N/A")):
      final_score = "N/A"

    FinalScore.text = "Malicious Score: " + str(final_score)
    Query_type = 'URL'

    """Add search to history"""
    self.Add_To_History(entry,                 VirusTotal_Score,
AbuseIPDB_Score,      X_Force_Exchange_Score,      final_score,
Query_type)

    """Visual indication for search completion"""
    ProgressBar.value = 100

    return


  """Gets Risk for URL from VT API"""
  def     get_VT_Risk_URL(self,     entry,     VirusTotal_JSON,
VirusTotal_Score, score):

    """In order to make successful requests with URL items to
the VirusTotal API the URL needs to first be encoded"""
    url_id                                                    =
base64.urlsafe_b64encode((entry.text).encode()).decode().strip(
"=")

    """Making request to the API and capturing its response - At
the same the API Key is sent in the header for authentication
resons"""
    response                =                requests.get(url=
'https://www.virustotal.com/api/v3/urls/'       +       url_id,
headers={"x-
apikey":"eb030a8bdb7c29588aec133be486853191b59d9805a9baa4b9dd9d
9099a61eaa"})

    """ If the Api returns a valid response calculate the score
else print "N/A" """
    if response.status_code == 200:
      json_response = response.json()
      uglyjson = response.json()
      VirusTotal_JSON.text   =(json.dumps(uglyjson,   indent=2,
sort_keys=True))
      data = json_response["data"]
```

```
      for key,value in data.items():
        if key=='attributes':
          attributes=value

      for key,value in attributes.items():
        if key=='last_analysis_stats':
          last_analysis_stats=value

      for key,value in last_analysis_stats.items():
        if key =='harmless':
          harmless=value
        if key =='malicious':
          malicious=value
        if key =='suspicious':
          suspicious=value
        if key =='timeout':
          timeout=value
        if key =='undetected':
          undetected=value


      #total = harmless + malicious + suspicious
      """The following formula converts the Virustotal Score to
{0,10} range"""
      finalRisk =(malicious * 10) + (suspicious * 5)
      if finalRisk>100:
        finalRisk = 100

      score = round((finalRisk/10),1)
      self.getScore(VirusTotal_Score, score)
    else:

      VirusTotal_JSON.text = "N/A"
      VirusTotal_Score.text_color = (130/255,130/255,130/255,1)
      VirusTotal_Score.text = "N/A"

    return score


  """Gets Risk for URL from AbuseIpDB API""" #Note that the
AbuseIPDB Api does not support URL searching so we will have a
value of N/A as a result
  def   get_AbuseIpDB_Risk_URL(self,   entry,   AbuseIPDB_JSON,
AbuseIPDB_Score, score):
    score = 0
    AbuseIPDB_Score.text_color = (130/255,130/255,130/255,1)
    AbuseIPDB_Score.text = "N/A"
    AbuseIPDB_JSON.text = "N/A"

    return

  """Gets Risk forURL from xForce API"""
```

```
  def   get_XFE_Risk_URL(self,   entry,   X_FORCE_EXCHANGE_JSON,
X_Force_Exchange_Score, score):

    """Making request to the API and capturing its response - At
the same useing basic_authentication to authenticate ourselves
to the API"""
    response                                                    =
requests.get('https://api.xforce.ibmcloud.com/url/'           +
entry.text,        auth=HTTPBasicAuth('ab51ab4e-90ac-4637-80ad-
4d297981c6d8', 'cd23e237-e38c-4378-9e0c-500c1b316893'))

    """ If the Api returns a valid response calculate the score
else print "N/A" """
    if response.status_code == 200:
      json_response = response.json()
      uglyjson = response.json()
      X_FORCE_EXCHANGE_JSON.text         =(json.dumps(uglyjson,
indent=2))

      """The following formula determines the X-FORCE Score"""
      result = json_response["result"]
      for key, value in result.items():
        if key=="score":
          score = int(value)
      score = round((score*10)/10,1)
      self.getScore(X_Force_Exchange_Score, score)
    else:
      X_FORCE_EXCHANGE_JSON.text = "N/A"
      X_Force_Exchange_Score.text_color                         =
(130/255,130/255,130/255,1)
      X_Force_Exchange_Score.text = "N/A"

    return score

  """Clears/Initializes the fields of textbox and results when
the recyvle icon on the top right is clicked"""
  def  new_Search(self,  entry,VirusTotal_JSON,  AbuseIPDB_JSON,
X_FORCE_EXCHANGE_JSON,    VirusTotal_Score,    AbuseIPDB_Score,
X_Force_Exchange_Score, Home, FinalScore, ProgressBar):

    VirusTotal_Score.text = ""
    AbuseIPDB_Score.text= ""
    X_Force_Exchange_Score.text = ""
    VirusTotal_JSON.text= ""
    AbuseIPDB_JSON.text= ""
    X_FORCE_EXCHANGE_JSON.text= ""
    entry.text = ""
    FinalScore.text="Malicious Score: "
    ProgressBar.value = 0
    return
```

```
  """Clears/Initializes the fields of textbox and results before
the execution for the next search so that the user has visual
indication that he initiated the search"""
  def        manual_Search(self,        entry,VirusTotal_JSON,
AbuseIPDB_JSON,     X_FORCE_EXCHANGE_JSON,     VirusTotal_Score,
AbuseIPDB_Score,   X_Force_Exchange_Score,   Home,   FinalScore,
ProgressBar):
    VirusTotal_Score.text = ""
    AbuseIPDB_Score.text= ""
    X_Force_Exchange_Score.text = ""
    VirusTotal_JSON.text= ""
    AbuseIPDB_JSON.text= ""
    X_FORCE_EXCHANGE_JSON.text= ""
    FinalScore.text="Malicious Score: "
    ProgressBar.value = 0

    return

  """Adds the last search in the History tabb"""
  def     Add_To_History(self,     entry,     VirusTotal_Score,
AbuseIPDB_Score,      X_Force_Exchange_Score,      final_score,
Query_type):

    """The followin piece of code constructs a Dictionary that
will hold all the information/results that will be then be
saved/written in the HISTORY tab"""
    queryString          =          {'Searched_for':entry.text,
'Query_type':Query_type}
    engine_Dict                                                =
{'VirusTotal_Score':VirusTotal_Score.text,'AbuseIPDB_Score':Abu
seIPDB_Score.text,'XForceExchange_Score':X_Force_Exchange_Score
.text}
    data_Dict=                     {'Query_String':queryString,
'Absolute_API_Score':str(final_score),
'Engine_Score':engine_Dict}
    history_Dict = {'Last_Searched_Item': data_Dict}
    uglyjson = history_Dict
    History =(json.dumps(uglyjson, indent=3))

self.manager.get_screen('History').ids.History_Label.text=(self
.manager.get_screen('History').ids.History_Label.text).replace(
"Last_Searched_Item", "Previously_Searched_Item")
    self.manager.get_screen('History').ids.History_Label.text =
History      +      "\n"      +      "\n"+      "\n"      +
self.manager.get_screen('History').ids.History_Label.text

    return


  def hyperlink(self, tx):
    test                                                       =
self.manager.get_screen('homePage').ids.VirusTotal_Score.text
```

```
    history
=(self.manager.get_screen('History').ids.History_Label.text)

    if history != "" :
      found = False
      for i in range(78,len(history)):
        if history[i] == " " and found == False:
          k= i-3
          found = True

      last_Searched_Item = ""
      for i in range(79,k):
        #print (history[i], end = "")
        last_Searched_Item = last_Searched_Item + history[i]


      if last_Searched_Item != "" and test != "":
        if tx == "VirusTotal":

webbrowser.open("https://www.virustotal.com/gui/search/"      +
last_Searched_Item)
        elif tx == "AbuseIPDB_Score":
          webbrowser.open("https://www.abuseipdb.com/check/"  +
last_Searched_Item)
        elif tx == "X_Force_Exchange_Score":

webbrowser.open("https://exchange.xforce.ibmcloud.com/search/"
+ last_Searched_Item)
      return
    return


class SecondWindow(Screen):
  pass

class ThirdWindow(Screen):
  pass

class FourthWindow(Screen):
  pass

class FifthWindow(Screen):
  pass

class WindowManager(ScreenManager):
  pass

class Absolute_APIApp(MDApp):

  class ContentNavigationDrawer(BoxLayout):
    pass

  class DrawerList(ThemableBehavior, MDList):
```

```
    pass

  def on_start(self):
    pass

  """The build function is the function that returns the kv tha
determines how the front_end part of the app will be displayed"""
  def build(self):

    kv = Builder.load_string(screen_helper)
    self.theme_cls.theme_style = "Light"
    self.theme_cls.primary_palette = "Blue" #""" "DeepPurple",
"Pink"""

    """['Red', 'Pink', 'Purple', 'DeepPurple', 'Indigo', 'Blue',
'LightBlue', 'Cyan', 'Teal', 'Green',
    #'LightGreen',   'Lime',   'Yellow',   'Amber',   'Orange',
'DeepOrange', 'Brown', 'Gray', 'BlueGray']"""

    """self.theme_cls.primary_hue = "800"
    #['50', '100', '200', '300', '400', '500', '600', '700',
'800', '900', 'A100', 'A200', 'A400', 'A700']"""

    return kv
if __name__== "__main__":
  Absolute_APIApp().run()
"""#$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$$$$$$$#$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$$$$$$$$$$"""
```