Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάλυση Κακόβολου Λογισμικού σε Android** **Android Malware Analysis**
Ονοματεπώνυμο Φοιτητή	**Κοσσιαράς Φώτης**
Πατρώνυμο	**Βασίλειος**
Αριθμός Μητρώου	**ΜΠΣΠ_15099**
Επιβλέπων	**Πατσάκης Κωνσταντίνος , Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Οκτωβρίου 2018**

Πίνακας περιεχομένων

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Πατσάκης Κωσταντίνος Επίκουρος Καθηγητής	Αλέπης Ευθύμιος Επίκουρος Καθηγητής	Τσιχριντζής Γεώργιος Καθηγητής

Περίληψη

Το malware είναι η λέξη που ξεχωρίζει για τις λέξεις "malicious software" δηλαδή κακόβουλο λογισμικό. Το κακόβουλο λογισμικό είναι ένας όρος ομπρέλα για διάφορους τύπους κακόβουλων προγραμμάτων που έχουν σχεδιαστεί από κυβερνητικούς εγκληματίες. Σήμερα, όλο και περισσότεροι χρήστες στο διαδίκτυο γίνονται θύματα επιθέσεων στον κυβερνοχώρο και στοχεύουν επίσης οργανώσεις αμετάβλητες στο μέγεθος τους.

Τα κακόβουλα προγράμματα παρέχουν είσοδο backdoor σε υπολογιστικές συσκευές για κλοπή προσωπικών πληροφοριών, εμπιστευτικά δεδομένα και πολλά άλλα.

Όπως προαναφέρθηκε, οι επιθέσεις κακόβουλου λογισμικού συνεχώς αυξάνονται καθημερινά, συνεπώς, υπάρχει μια σκληρή ανάγκη για τη διεξαγωγή ανάλυσης κακόβουλου λογισμικού για την κατανόηση των τύπων, της φύσης, των μεθοδολογιών επίθεσης κ.λπ.

Σκοπός της διπλωματικής εργασίας αποτελεί η κατανόηση βασικών εννοιών ασφάλειας που σχετίζονται με εφαρμογές, οι οποίες υποστηρίζονται από το λειτουργικό σύστημα android. Επιπλέον, η στατική ανάλυση, οι μέθοδοι καθώς επίσης και τα εργαλεία τα οποία χρησιμοποιούνται θα βοηθήσουν ώστε να γίνουν αυτές οι έννοιες οικείες.

Abstract

Malware is the singly coined word for the words “Malicious Software”. Malware is an umbrella term for various types of malicious programs designed by cybercriminals. Today, more and more online users are becoming victims of cyber attacks and organizations invariable of their size are also being targeted.

The malicious programs provide backdoor entry into computing devices for stealing personal information, confidential data, and much more.

As mentioned above, the malware attacks are constantly increasing day by day, so, there is a dire need to conduct malware analysis to understand their types, nature, attacking methodologies, etc

The aim of the diploma thesis is to understand basic security concepts related to applications, which are supported by the android operating system. In addition, static analysis, methods as well as the tools used will help to make these concepts familiar.

ΕΙΣΑΓΩΓΗ

ΤΙ ΕΊΝΑΙ ΤΟ ANDROID

Το πιο δημοφιλές λειτουργικό σύστημα για συσκευές κινητής τηλεφωνίας είναι το Android, το όποιο “τρέχει” τον πυρήνα του λειτουργικού Linux. Αρχικά αναπτύχθηκε από την Google και αργότερα από την [Handset Alliance|Open Handset Alliance]. Η πρώτη έκδοση του λειτουργικού αυτού κυκλοφόρησε το Σεπτέμβρη του 2008 ενώ αναβαθμίζεται τακτικά μέχρι και σήμερα. Το Android είναι σχεδιασμένο ειδικά για συσκευές με οθόνη αφής και επιτρέπει στους προγραμματιστές εφαρμογών τη χρήση της γλώσσας προγραμματισμού Java, ελέγχοντας τη συσκευή μέσω βιβλιοθηκών λογισμικού της Google.

Το Android είναι το πιο ευρέως διαδεδομένο λογισμικό στον κόσμο. Οι συσκευές με Android έχουν περισσότερες πωλήσεις από όλες τις συσκευές Windows, IOS και Mac OS X μαζί. Πολλές κατασκευαστικές εταιρίες κινητών τηλεφώνων πλέον χρησιμοποιούν το λειτουργικό Android για τα smartphones τους, μερικές από αυτές είναι η LG, Samsung, HTC, Lenovo, Sony Ericsson, Xiaomi κ.α. Ένα βασικό προνόμιο των συσκευών που “τρέχουν” το λογισμικό αυτό είναι πως είναι αφενός multimedia (παρέχεται δηλαδή η δυνατότητα να αναπαραχθούν πολλά μέσα) και multitasking (όπου δίνεται η δυνατότητα εκτέλεσης πολλών εφαρμογών ταυτόχρονα όπως για παράδειγμα να υποστηρίζεται η αναπαραγωγή μουσικής ταυτόχρονα με την αποστολή μηνύματος χωρίς να χρειάζεται να τερματιστεί κάποια από τις δύο). Η περιήγηση στο διαδίκτυο είναι ταχύτατη με δυνατότητα επιλογής browsers που υποστηρίζουν και flash. Ανεξάρτητα από το κόστος της συσκευής, όλες διαθέτουν GPS και Wi-fi, δικαιώνοντας έτσι το βασικό λόγο δημιουργίας του εν λόγω λειτουργικού συστήματος που δεν είναι άλλος παρά η ανεμπόδιστη και εύκολη πρόσβαση στο διαδίκτυο, σε συνδυασμό με ένα πλήθος εφαρμογών (apps), όπως χάρτες, αναζήτηση, chat και e–mail, που πραγματικά επιτρέπουν στο χρήστη να μένει διαρκώς δικτυωμένος και ενημερωμένος. Βασικό χαρακτηριστικό του Android, επίσης, είναι η πληθώρα εφαρμογών που διατηρούν τη συνεχή σύνδεση με Facebook, MySpace, Twitter και δεκάδες άλλες υπηρεσίες social networking. Ακόμη, το Android δίνει τη δυνατότητα να προσθήκης widget, δηλαδή εικονίδια για την ταχύτερη πρόσβαση στα προγράμματα, τα οποία τοποθετούνται στη home screen του κινητού (launcher). [1][2]

ΑΡΧΙΤΕΚΤΟΝΙΚΉ ΚΑΙ ΑΠΕΙΛΈΣ ΛΕΙΤΟΥΡΓΙΚΟΎ ΣΥΣΤΉΜΑΤΟΣ ANDROID

Η αρχιτεκτονική του λειτουργικού συστήματος Android είναι καλά διαδεδομένη, που περιλαμβάνει τον πυρήνα του Linux, τις βιβλιοθήκες, το application framework, εφαρμογές,και το περιβάλλον Virtual Machine του Dalvik (DVM). Για να αποκτήσετε "root" σε μια συσκευή πρέπει να αποκτήσεις πρόσβαση στον πυρήνα του Linux που τρέχει μια συσκευή Android. Τα περισσότερα κακόβουλα προγράμματα Android δεν επιχειρούν να πραγματοποιήσουν exploits για να πάρουν root, καθώς αυτό δεν απαιτείται για κακόβουλα κίνητρα. Αντίθετα, οι εφαρμογές είναι συνήθως τροποποιημένες για να προστεθεί ένα κρυφό Trojan έτσι ώστε όταν ο χρήστης εγκαθιστά μια εφαρμογή, το Trojan είναι επίσης εγκατεστημένο. Μόλις εγκατασταθεί και τρέξει, το κακόβουλο λογισμικό μπορεί να χρησιμοποιήσει μια ευρεία ποικιλία δικαιωμάτων που επιτρέπονται στην εφαρμογή για να στείλει στη συνέχεια μηνύματα κειμένου, για τις πληροφορίες τηλεφώνου και γεωγραφικής κατανομής να διαχειρίζεται και να παρακολουθεί όλα τα είδη επικοινωνιών και πολλά άλλα.

Η αποκτηση πρόσβασης root στον πυρήνα του Linux σε ένα Android λειτουργικό σύστημα, μπόρει να πραγματοποιηθεί με διάφορες μέθοδους. Αυτό μπορεί να είναι χρήσιμο για έναν αναλυτή σε διάφορες καταστάσεις, αλλά μπορεί επίσης να περιλαμβάνει νομικές εκτιμήσεις για τον αναλυτή και τη χώρα εργασίας που απαιτούν διάκριση και νομική επανεξέταση πριν πραγματοποιήσει τέτοιες ενέργειες σε μια συσκευή. Για παράδειγμα, κάποιο κακόβουλο λογισμικό Android προσπαθεί να εκτελέσει ένα exploit για να αποκτήσει root σε μια συσκευή, αναγκάζοντας έναν αναλυτή να είναι εξοικειωμένος με όλα αυτά τα exploits και πώς να ερευνά και να ανταποκρίνονται σε μια τέτοια απειλή.

Επιπλέον, ένας ερευνητής ή ένας νομικός μπορεί να χρησιμοποιήσει ένα exploit για να αποκτήσει πρόσβαση σε μια συσκευή που διαφορετικά θα ήταν αδύνατο. Πάρτε για παράδειγμα μια συσκευή που προστατεύεται με κωδικό πρόσβασης από ένα αποθανών πρόσωπο, όπου τα μέλη της οικογένειας ενδέχεται να επιθυμούν τη λήψη φωτογραφιών και άλλων πληροφοριών από τη συσκευή. Κάποια εμπορικά πακέτα περιλαμβάνουν rooting exploits ως μέρος μιας λύσης για την υποστήριξη forensic access και έρευνας στο τηλέφωνο.

Το rooting τυπικά λειτουργεί μόνο για συγκεκριμένες συσκευές ή για λειτουργικά συστήματα και διαμορφώσεις που συνήθως καλύπτονται γρήγορα για να περιορίσουν την έκθεση σε κίνδυνο. Όπως είναι γνωστό τα exploits για Android που χρησιμοποιούνται για να πάρει κάποιος δικαιώματα root για διάφορες εκδόσεις του Android λειτουργικού συστήματος είναι τα ακόλουθα: RageInTheCage, Exploid (CVE-2009-1185),GingerBreak (CVE-2011-1823) και ZergRush (CVE-2011-3874).[3]

ΕΠΙΚΊΝΔΥΝΕΣ ΕΦΑΡΜΟΓΈΣ

Με την γρήγορη υιοθέτηση και ανάπτυξη εφαρμογών και λύσεων χρησιμοποιώντας το λειτουργικό σύστημα Android, τώρα υπάρχει ένα τεράστιο ποσό από αγαθά για τις κινητές συσκευές. Αυτά τα αγαθά παρουσιάζουν μεγάλο ενδιαφέρον για τους κακόβουλους καθώς μπρούν να τις εκμεταλλευτούν με μια ποικιλία μέσων και κινήτρων. Πολλοί χρήστες τέτοιων συσκευών απολαμβάνουν το πόσο πολλά πράγματα μπορούν να κάνουν (functionality) αλλά δεν συνειδητοποιήσουν ή σταματούν να εξετάζουν πόσα στοιχεία είναι στην πραγματικότητα σε μια κινητή συσκευή. Υπάρχουν εφαρμογές για την ανασυγκρότηση των τρισδιάστατων απεικονίσεων του δωματίου, υπενθυμίσεις προσευχής, συνταγές, μουσική και πολλά άλλα.

Οι κινητές συσκευές είναι τόσο ισχυρές και ολοκληρωμένες ώστε να σου παρέχουν διαθέσιμες, περισσότερες πληροφορίες από ότι συνειδητοποιούν οι περισσότεροι χρήστες. Φανταστείτε ότι η συσκευή σας συμβιβάζεται, τραβώντας φωτογραφίες από εσάς και βλέποντας τα πάντα χωρίς τη γνώση ή τη συγκατάθεσή σας. Αυτό βοηθά στην απεικόνιση της άκρης του παγόβουνου όσον αφορά τον τύπο της πληροφόρησης, καθώς και το σχεδιασμό και τον έλεγχο σε ευαίσθητα

δεδομένα που μπορεί κανείς να αποκτήσει από μια κινητή συσκευή που συνδέεται τυπικά σε έναν ενήμερο χρήστη καθώς ζουν τη ζωή τους. Διαφορετικοί τύποι κακοποιών παραγόντων έχουν πλούσια εργαλεία για πρόσβαση σε μια κινητή συσκευή. Για παράδειγμα, οι ηλεκτρονικοί εγκληματίες μπορούν να κερδίσουν χρήματα μέσω κλήσεων και κειμένου σε γραμμές premium και υπονομεύουν το two-factor banking authentication.

Οι φορείς κατασκοπείας μπορούν να παρακολουθήσουν τη φυσική θέση ενός στόχου και να έχουν πρόσβαση σε τεράστιο όγκο ευαίσθητων πληροφοριών και τις επαφές σε μια κινητή συσκευή. Οι hacktivists μπορούν να έρθουν σε επαφή με άλλους ακτιβιστές καθώς γρήγορα μπορούν να ξεσηκώσουν διαμαρτυρίες για τη χρησιμοποίηση των κινητών συσκευών. Οι καταναλωτές σε χώρες όπου η ελευθερία του λόγου και τα ανθρώπινα δικαιώματα είναι καταπιεσμένα συχνά διαπιστώνουν ότι μια κινητή συσκευή είναι το μόνο κύριο μέσο όπου μπορούν να επικοινωνούν μεταξύ τους και με τον ελεύθερο κόσμο μαζικά. Αυτές είναι μερικές από τις πολύ δυνατές εφαρμογές όπου κάνουν κατάχρηση όσοι απασχολούνται σε διάφορες ομάδες κακοποιών και έχουν συμφέροντα σε συνδεόμενες συσκευές που υποστηρίζονται από Android.

Μια ενδιαφέρουσα εξέλιξη είναι πώς οι διαφημιζόμενοι συλλέγουν πληροφορίες για να παρακολουθούν τις συνήθειες των χρηστών. Για παράδειγμα, το Latest Nail Fashion Trends 3.1 παρακολουθεί τον γεωγραφικό εντοπισμό των χρηστών. Περίπου 7 τοις εκατό ή περισσότερες εφαρμογές Android διαβάζουν επίσης τη λίστα επαφών όπως το Longman Contemporary English 1.81. Ακόμη περισσότερες εφαρμογές ενδέχεται να διαρρεύσουν ένα αναγνωριστικό συσκευής / IMEI όπως τα Football Games—Soccer Juggle 1.4.2. Μην ξεχνάτε το ηλεκτρονικό ταχυδρομείο, με το Logo Quiz Car Choices 1.8.2.9 διαρρέοντας την πληροφοριά από τον κατασκευαστή του λογισμικού. Επόμενος είναι ο αριθμός τηλεφώνου και ούτω καθεξής πολλές εφαρμογές με τόσες άδειες που δεν είναι απαραίτητες και συχνά δεν επιτράπηκαν από τους καταναλωτές που εγκαθιστούν τέτοιες εφαρμογές.[3]

ΣΤΑΤΙΚΉ ΑΝΆΛΥΣΗ

Ο προσδιορισμός εάν ένα ύποπτο αρχείο είναι κακόβουλο συνήθως αρχίζει με στατική ανάλυση. Η στατική ανάλυση δεν συνεπάγεται την εκτέλεση του κώδικα ή το άνοιγμα ενός αρχείου (δυναμική ανάλυση), ή αντίστροφη μηχανική του κώδικα μέσω disassembly ή debugging.Η στατική ανάλυση περιλαμβάνει σε μεγάλο βαθμό την ταυτοποίηση και την αναζήτηση κρυπτογραφικών τιμές κατακερματισμού, όπως MD5, συμβολοσειρές και μεταδεδομένα. Πιο σημαντικό, η στατική ανάλυση αποτελεί μέρος μιας ευρύτερης διαδικασίας που είναι αναδρομική από τη φύση της, όπως η εξαγωγή αρχείων κλάσης από ένα εχθρικό APK και στη συνέχεια η συλλογή στατικών τα δεδομένα για μεμονωμένα αντικείμενα, εξετάζοντας τη στατική ανάλυση των σχετικών APK, και ούτω καθεξής, καθώς ο αναλυτής επιδιώκει να καθιερώσει περισσότερο το πλαίσιο και την αναλυτική σχέσεις για την αξιολογική αρχή στην κατανόηση μιας απειλής.

Η στατική ανάλυση είναι το πιο ευέλικτο τμήμα της ανάλυσης κακόβουλου λογισμικού Android καθώς μπορεί να εκτελεστεί από ένα πλήθος λειτουργικών συστημάτων παρά από το να εξαρτάται από το λειτουργικό σύστημα Android. Πολλοί αναλυτές προτιμούν να αναπτύξουν ένα σύνολο εργαλείων και σεναρίων μέσα σε ένα Linux περιβάλλον, όπως το Ubuntu, λόγω της ασφάλειας που παρέχει το λειτουργικό σύστημα, εγγενείς λύσεις για δέσμες ενεργειών (Python, Perl, Bash) και ευρεία ποικιλία εργαλείων που μπορούν εύκολα να χρησιμοποιηθούν σε ένα τέτοιο περιβάλλον για αποτελεσματική στατική ανάλυση κακόβουλου λογισμικού.

Η διαδικασία στατικής ανάλυσης του κακόβουλου λογισμικού Android είναι η ίδια όπως αυτή των παραδοσιακών Windows, Linux ή άλλων ειδών κακόβουλου λογισμικού. Αυτό που διαφέρει για τις απειλές του Android είναι ο τρόπος δημιουργίας των αρχείων APK και το πως μεταγλωττίζονται σε σύγκριση με εκείνη ενός binary αρχείου Windows. Τα δυαδικά αρχεία των Windows

συντάσσονται ως εκτελέσιμα με μια κεφαλίδα MZ. Οι εφαρμογές Android έχουν εκπονηθεί ως APK που μπορούν να αποσυσκευαστούν σε ξεχωριστά αρχεία συμπεριλαμβανομένων τον

πηγαίο κώδικα, το manifest και άλλα αρχεία που είναι κοινά σε ένα APK αρχείο. Οι Αναλυτές που είναι εξοικειωμένοι με τη στατική ανάλυση άλλων τύπων κακόβουλου λογισμικού θα προσαρμοστούν γρήγορα στην εκτέλεση στατικής ανάλυσης κακόβουλου λογισμικού Android. Αξιοσημείωτο είναι ότι η στατική ανάλυση μπορεί και θα πρέπει να είναι αυτοματοποιημένη, όπως ένα σενάριο Python ή ένα εργαλείο για την δημιουργία κατακερματισμού δεδομένων για πολλά αρχεία.[3]

Εργαλεία - Πλατφόρμες -Ιστοσελίδες

GOOGLE PLAY

Το Google Play είναι η επίσημη αγορά για εφαρμογές Android. Η εφαρμογή η ίδια ονομάζεται Google Play σε συσκευές, διατίθεται στο παρακάτω δικτυακό τόπο (https://play.google.com/store). Οι χρήστες μπορούν να κατεβάσουν εύκολα οποιαδήποτε εφαρμογή ενδιαφέροντος από τον ιστότοπο, με μερικές να είναι ελεύθερες και άλλες εμπορικά αναπτυγμένες εφαρμογές. Ωστόσο,τα δικαιώματα μέσω της Google Play διαφέρουν ανάλογα με τη λειτουργία και τη γεωγραφική θέση, όπως τηλεοπτικές εκπομπές που διατίθενται μόνο για μικρό αριθμό χωρών. Όλες οι χώρες μπορούν να ενεργοποιήσουν την αγορά εφαρμογών μέσω του Google Play αλλά επιλέγοντας χώρες που υποστηρίζονται για τους προγραμματιστές που μπορούν να πουλήσουν εφαρμογές μέσω της αγοράς (https://support.google.com/googleplay/android-developer / table3539140? Rd = 1). Στις πρώτες μέρες χρησιμοποιήθηκαν λογαριασμοί προγραμματιστών για τη διανομή εχθρικών εφαρμογών μέσω της επίσημης αγοράς, όπως το περίφημο DroidDream με τουλάχιστον τρεις αδίστακτους λογαριασμούς και δεκάδες εχθρικές εφαρμογές, οι οποίες εξαπλώθηκαν στην αγορά το 2011. Βελτιωμένοι έλεγχοι ασφαλείας ακολούθησαν τέτοιες εκδηλώσεις, με τους απατεώνες να υπονομεύουν τώρα λογαριασμούς προγραμματιστών ή κώδικα διάδοσης μέσω άλλων μέσων, όπως ανεπίσημα "crack" sites, διανέμοντας δημοφιλείς εφαρμογές που ενδιαφέρουν τους καταναλωτές.

CONTAGIO MOBILE

Η Mila Parkour διατηρεί ένα από τα πιο δημοφιλή και ενημερωμένα ιστολόγια στο Διαδίκτυο παρέχοντας και τα δύο δείγματα και συνδέσμους προς ανάλυση για κάθε δείγμα. Ο Parkour χρησιμοποιεί ένα ιδιόκτητο αλλά το προσφέρει σε άτομα που την ρωτούν πληροφορίες για την αποκρυπτογράφηση λήψεων από τον ιστότοπό της. Κύλιση προς τα κάτω η σελίδα στη δεξιά πλευρά προσφέρει μια μακρά λίστα δειγμάτων που οργανώνονται με το όνομα της οικογένειας, όπως το opfake, το Plankton, το Stel και άλλοι.http://contagiominidump.blogspot.com/

SOOT

Το Soot είναι προϊόν της ερευνητικής ομάδας του Sable από το πανεπιστήμιο McGill, του οποίου στόχος είναι η παροχή εργαλείων που οδηγούν στην καλύτερη κατανόηση και ταχύτερη εκτέλεση προγραμμάτων Java. Ο ιστότοπος Soot βρίσκεται στη διεύθυνση http: //www.sable.mcgill.ca/soot/. Το Soot παρέχει πολλά διαφορετικά γραφήματα ροής ελέγχου (CFG) στο πακέτο soot.toolkits.graph. Στη βάση αυτών των γραφημάτων βρίσκεται η διεπαφή DirectedGraph ορίζει τις μεθόδους για τη λήψη: τα σημεία εισόδου και εξόδου στο γράφημα, οι διάδοχοι και προκάτοχοι ενός δεδομένου κόμβου, ένα iterator για την επανάληψη του γραφήματος σε κάποια αόριστη σειρά και το μέγεθος γραφημάτων (αριθμός κόμβων). Η βασική κλάση για αυτά τα είδη γραφημάτων είναι η UnitGraph, μια αφηρημένη κλάση που παρέχει εγκαταστάσεις για την κατασκευή CFG.

- Soot-Infoflow

- Soot-Infoflow-Android
- Soot-Trunk [4]

ELASTIC SEARCH

Το Elastic Search (ES) είναι μια κατανεμημένη και άκρως διαθέσιμη μηχανή αναζήτησης ανοιχτού κώδικα που είναι χτισμένη πάνω από το Apache Lucene. Είναι ένα open-source που είναι ενσωματωμένο σε Java και έτσι διατίθεται σε πολλές πλατφόρμες. Αποθηκεύετε μη δομημένα δεδομένα σε μορφή JSON, τα οποία επίσης καθιστούν μια βάση δεδομένων NoSQL. Έτσι, σε αντίθεση με άλλες βάσεις δεδομένων NoSQL, η ES παρέχει επίσης δυνατότητες μηχανών αναζήτησης και άλλα συναφή χαρακτηριστικά.https://www.elastic.co/.[5]

Εγκατάσταση

ΕΓΚΑΤΆΣΤΑΣΗ JAVA

Η *Java* είναι μια πολύ δημοφιλής γλώσσα αντικειμενοστραφή προγραμματισμού . Πολλές φορές , ακόμα και αν δεν θέλουμε να χρησιμοποιήσουμε άμεσα την Java , υπάρχουν εφαρμογές που για να εγκατασταθούν και να λειτουργήσουν χρειάζονται να την έχουμε ήδη εγκατεστημένη στο σύστημα μας .

Παρακάτω θα δούμε διάφορους τρόπους για να κάνουμε την εγκατάσταση της Java , στα Debian 8 .

Πριν την εγκατάσταση

Θα χρειαστούμε :

•Έναν Debian 8 Server

•Έναν non-root-sudo λογαριασμό χρήστη

Εγκατάσταση του Default JDk/JRE

Ο πιο εύκολος τρόπος να εγκαταστήσουμε την Java είναι χρησιμοποιώντας την version που έρχεται μάζι με το Debian .

Πρώτα κάνουμε update το package index :

```
sudo apt-get update
```

Και εγκαθιστούμε το JRE(Java runtime environment)

```
sudo apt-get install default-jre
```

Μπορούμε επίσης να εγκαταστήσουμε το JDK(java development kit) . Το JDK χρειάζεται μόνο αν θα κάνουμε compile java προγράμματα η αν το απαιτεί συγκεκριμένα κάποια εφαρμογή .

```
sudo apt-get install default-jdk
```

Εγκατάσταση του Oracle JDK

Αν θέλουμε να εγκαταστήσουμε το official version της Java που διανέμεται από την Oracle , πρέπει να κάνουμε και μερικά έξτρα βήματα .

Προσθέτουμε το repository στο source της apt get:

```
sudo add-apt-repository "deb http://ppa.launchpad.net/webupd8team/java/ubuntu xenial main"
```

Κάνουμε update την apt get :

```
sudo apt-get update
```

‘Επειτα εγκαθιστούμε την έκδοση που θέλουμε . Την δεδομένη στιγμή , η τελευταία έκδοση είναι η 9 και θα εγκαταστήσουμε αυτή :

```
sudo apt-get install oracle-java9-installer
```

Διαχείρηση της Java

Σε έναν server είναι πολυ πιθανό να είναι εγκατεστημένες πολλές διαφορετικές εκδόσεις της Java . Για να ρυθμίσουμε ποια θα είναι η default για χρήση στο command line , θα εκτελέσουμε την εντολή :

sudo update-alternatives --config java

ΕΓΚΑΤΆΣΤΑΣΗ INTELLIJ IDEA

Το IntelliJ IDEA διατίθεται σε δύο εκδόσεις: Ultimate και Community. Η κοινοτική έκδοση είναι ένα έργο ανοιχτού κώδικα και είναι δωρεάν, αλλά έχει λιγότερα χαρακτηριστικά. Η Ultimate έκδοση είναι εμπορική και παρέχει ένα εξαιρετικό σύνολο εργαλείων και χαρακτηριστικών. Για λεπτομέρειες, ανατρέξτε στον πίνακα σύγκρισης των εκδόσεων.

Για να εγκαταστήσετε το IntelliJ IDEA

Κατεβάστε το IntelliJ IDEA για το λειτουργικό σας σύστημα.

Κάντε τα παρακάτω ανάλογα με το λειτουργικό σας σύστημα:

Windows:

Εκτελέστε την ιδέαIC.exe ή το αρχείο ιδεώνIU.exe που έχετε κατεβάσει.

Ακολουθήστε τις οδηγίες στον οδηγό εγκατάστασης.

macOS:

Κάντε διπλό κλικ στο αρχείο idea.d.dmg ή ideaIU.dmg που έχετε κατεβάσει για να βάλετε την εικόνα του δίσκου macOS.

Αντιγράψτε το IntelliJ IDEA στο φάκελο "Εφαρμογές".

Linux:

Αποσυμπιέστε το αρχείο idea.g.gz ή ideaIU.gz που έχετε κατεβάσει σε διαφορετικό φάκελο, αν ο τρέχων φάκελος Downloads δεν υποστηρίζει την εκτέλεση αρχείων:

tar xfz ideaIC.tar.gz ή ideaIU.tar.gz. <new_archive_folder>

Η συνιστώμενη θέση εγκατάστασης σύμφωνα με το πρότυπο ιεραρχίας συστήματος αρχείων (FHS) είναι / opt. Για παράδειγμα, είναι δυνατό να εισαγάγετε την ακόλουθη εντολή:

sudo tar xf - *. tar.gz -C / opt /

Μεταβείτε στον κατάλογο bin, για παράδειγμα:

cd / opt / - * / bin

Εκτελέστε idea.sh από τον υποκατάλογο bin.

ΕΓΚΑΤΆΣΤΑΣΗ SOOT

Βήμα 1

Μεταβείτε στο import project και επιλέξτε το αρχείο '.project' και κάντε κλικ στο OK. Για να αποκτήσετε το αρχείο .project, κλωνοποιήστε Soot GitHub repository.

Βήμα 2

Στη συνέχεια, επιλέξτε τον κατάλογο Soot

Βήμα 3

Import project from external model Eclipse

Βήμα 4

Επιλέξτε το πλαίσιο με ‘keep project and module file in’ και ‘project format ως ‘.idea'.

Σημείωση: Επειδή κρατάμε τα αρχεία του έργου στο '.idea' dir, όλα αυτά θα αγνοηθούν με τη γραμμή ".idea" στο .gitignore

Βήμα 5

Καταργήστε την επιλογή όλων των έργων, εκτός από το Soot. Τα μη ελεγμένα έργα σχετίζονται με το Eclipse plug-in.

Σημείωση: Η διαδρομή κατασκευής θα σπάσει. Το SDK Java πιθανότατα δεν θα αναγνωριστεί και κάποια jars ενδέχεται να λείπουν.

Βήμα 6

Αλλάξτε τη μορφή στο module dependecies storage στο IntelliJ IDEA, επομένως δεν θα χρειαστεί να τροποποιήσετε το αρχείο .classpath. Μπορείτε να διορθώσετε εύκολα το SDK επαναφέροντας το, το οποίο γίνεται στο επόμενο βήμα.

Βήμα 7

Μεταβείτε στο view και open module settings και Dependencies tab και επιλέξτε τη δικιά σας Java version.

Βήμα 8

Κατεβάστε τα ελλείποντα jars αρχεία:

heros.jar και jasminclasses.jar, που διατίθενται από τη διεύθυνση https://soot-build.cs.uni-paderborn.de/public/origin/develop/soot/ [Αυτή η θέση περιέχει τώρα το soot-trunk.jar το οποίο πρέπει να μεταφορτωθεί αντί και των δύο heros.jar και jasminclasses.jar. Το έργο θα εξακολουθήσει να καταρτίζεται και να τρέχει σε IntelliJ Idea]

ant.jar, είναι διαθέσιμο π.χ. στο http://mvnrepository.com/artifact/org.apache.ant/ant/1.9.2

java_cup.jar, διατίθεται από το Sable / jasmin repo στη διεύθυνση
https://github.com/Sable/jasmin/tree/master/libs
Βάλτε αυτά τα αρχεία σε ./libs_intellij έτσι ώστε να πάρει το .gitignore.

ΕΓΚΑΤΆΣΤΑΣΗ ELASTIC SEARCH

https://www.linode.com/docs/databases/elasticsearch/a-guide-to-elasticsearch-plugins/

Υλοποίηση

WORKFLOW

Η διαδικασία η οποία ακολουθείται είναι η εξής:

Αρχικά “τρέχουμε” τον αυτοματοποιημένο αλγόριθμο (automate.sh) για κάθε κατηγορία εφαρμογών που έχουν οριστεί (benign/malicious). Στην συνέχεια αφού συγκεντρώσουμε τα callgraph για κάθε κατηγορία εφαρμογών τα τοποθετούμε σε συγκεκριμένους φακέλους. Τρέχοντας τον αλγόριθμο CG_DOC αναπαράγουμε τον αυτοματοποιημένο αλγόριθμο (index.sh). Καθώς εκτελείται από την γραμμή εντολών το συγκεκριμένο script ευρετηριοποιούμε αυτόματα τα δεδομένα που έχουν συγκεντρωθεί μέσα στο elastic search. Τέλος, με την εκτέλεση του αλγορίθμου CG_CLASSIFY πραγματοποιούμε αναζήτηση με το callgraph μιας άγνωστης εφαρμογής με σκοπό να κατηγοριοποιηθεί είτε ως benign ή malicious.

ΔΙΑΔΙΚΑΣΊΑ ΜΗΧΑΝΙΚΉΣ ΜΆΘΗΣΗΣ

Η υλοποίηση του αλγόριθμου APK_CG πραγματώθηκε χρησιμοποιώντας τις βιβλιοθήκες του Soot με τη βοήθεια των αρχείων soot-infoflow.jar, soot-infoflow-android.jar, soot-trunk.jar καθώς και των αρχείων SourceAndSinks.txt , Callbacks.txt . Η υλοποίηση αυτή είχε ως αποτέλεσμα την δημιουργία του γράφου (callgraph) για κάθε apk ξεχωριστά. Η διαδικασία αυτοματοποιήθηκε με δημιουργία του script (automate.sh) με σκοπό την δημιουργία γράφου για πολλαπλά apk. Προκειμένου να πραγματωθεί η διαδικασία μπορεί να εκτελεστεί το automate.sh με παράμετρο τα μονοπάτια, στα οποία εμπεριέχονται τα benign και malicious apks.

Για τη δημιουργία του ευρετηρίου index.sh χρειάστηκε η υλοποίηση του αλγορίθμου CG_DOC με σκοπό τη δημιουργία καινούριου ευρετηρίου καθώς και τη μαζική καταχώρηση των δεδομένων (callgraph) μέσα στο elasticsearch. Αφού αναπαραχθεί το συγκεκριμενο script,

χρειάζεται να το εκτελέσουμε μια φορά προκείμενου να έχουμε όλα τα δεδομένα μας ευρετηριοποιημένα.

ΔΙΑΔΙΚΑΣΊΑ ΚΑΤΗΓΟΡΙΟΠΟΊΗΣΗΣ

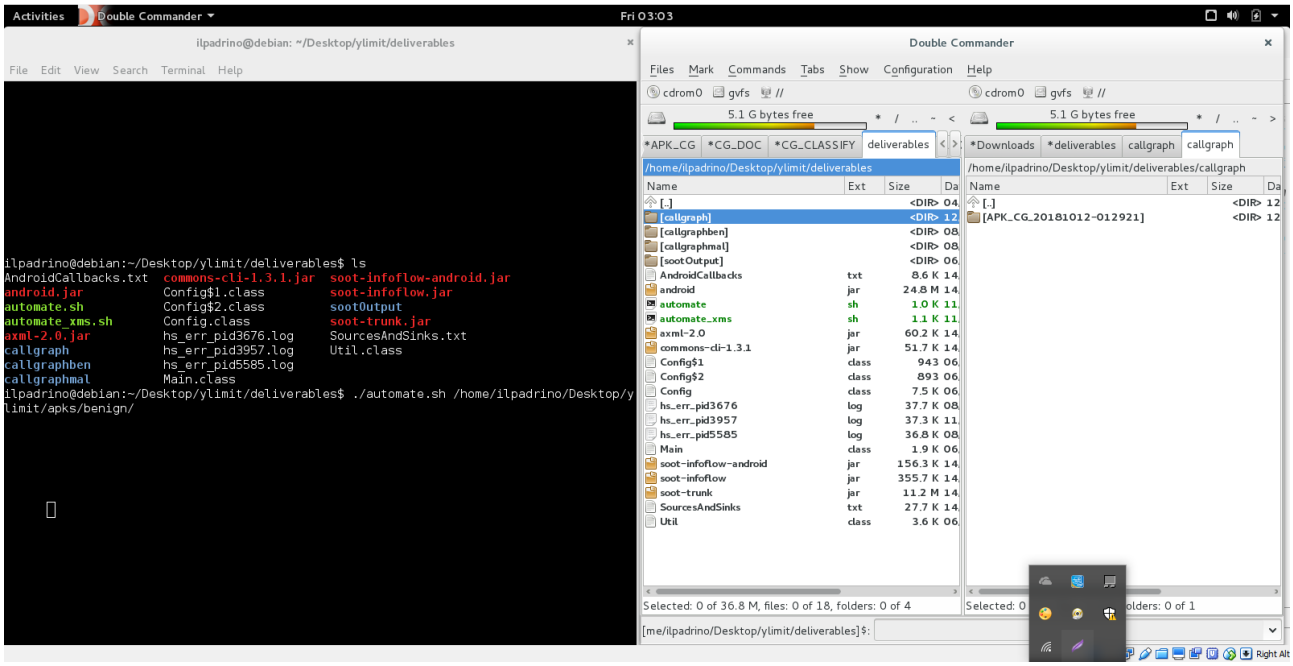
Η υλοποίηση του αλγόριθμου APK_CG πραγματώθηκε χρησιμοποιώντας τις βιβλιοθήκες του Soot με τη βοήθεια των αρχείων soot-infoflow.jar, soot-infoflow-android.jar, soot-trunk.jar καθώς και των αρχείων SourceAndSinks.txt , Callbacks.txt . Η υλοποίηση αυτή είχε ως αποτέλεσμα την δημιουργία του γράφου (callgraph) για κάθε apk ξεχωριστά. Η διαδικασία αυτοματοποιήθηκε με δημιουργία του script (automate.sh) με σκοπό την δημιουργία γράφου για πολλαπλά apk. Προκειμένου να πραγματωθεί η διαδικασία μπορεί να εκτελεστεί το automate.sh με παράμετρο τα μονοπάτια, στα οποίο είναι τοποθετημένο ένα άγνωστο apk.

Η κατηγοριοποίηση ενός άγνωστου apk μπορεί να επιτευχθεί με την εκτέλεση του αλγορίθμου CG_CLASSIFY δίνοντας σαν είσοδο το γράφο (callgraph) όπως δημιουργήθηκε σύμφωνα με το παραπάνω βήμα.

ΑΝΆΛΥΣΗ ΔΙΑΔΙΚΑΣΊΑΣ ΜΗΧΑΝΙΚΉΣ ΜΆΘΗΣΗΣ

Δημιουργία του callgraph για κάθε APK

Με εκτέλεση της εντολής παράγεται το callgraph για τα benign apks :
./automate.sh /home/ilpadrino/Desktop/ylimit/apks/benign/
Ομοιως αλλα με διαφορετικο μονοπατι για τα malicious apks:
./automate.sh /home/ilpadrino/Desktop/ylimit/apks/malicious/

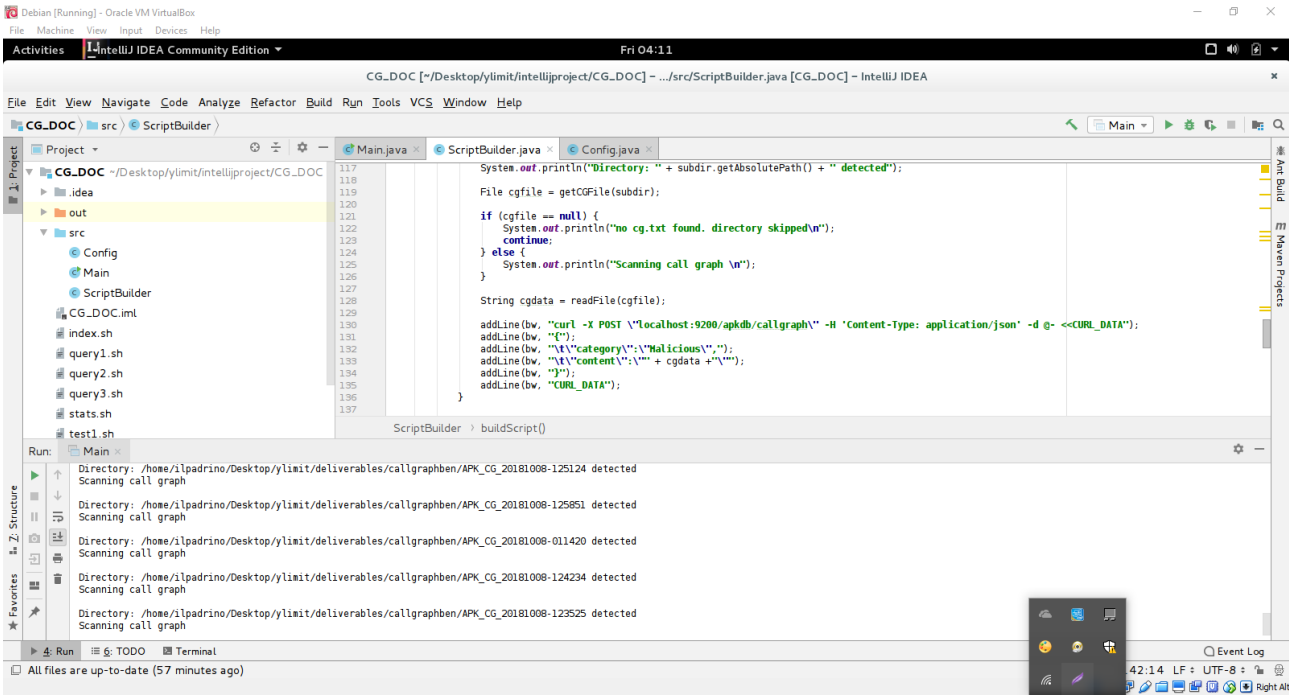


Δημιουργία index.sh

Ο αλγόριθμος CG_DOC συγκεντρώνει τα δεδομένα από τις δύο κατηγορίες (benign/malicious) τα οποία στη συνεχεία με κατάλληλη μορφοποίηση τα τοποθετεί στο εκτελέσιμο αρχείο μας (index.sh)

/home/ilpadrino/Desktop/ylimit/deliverables/callgraphben/

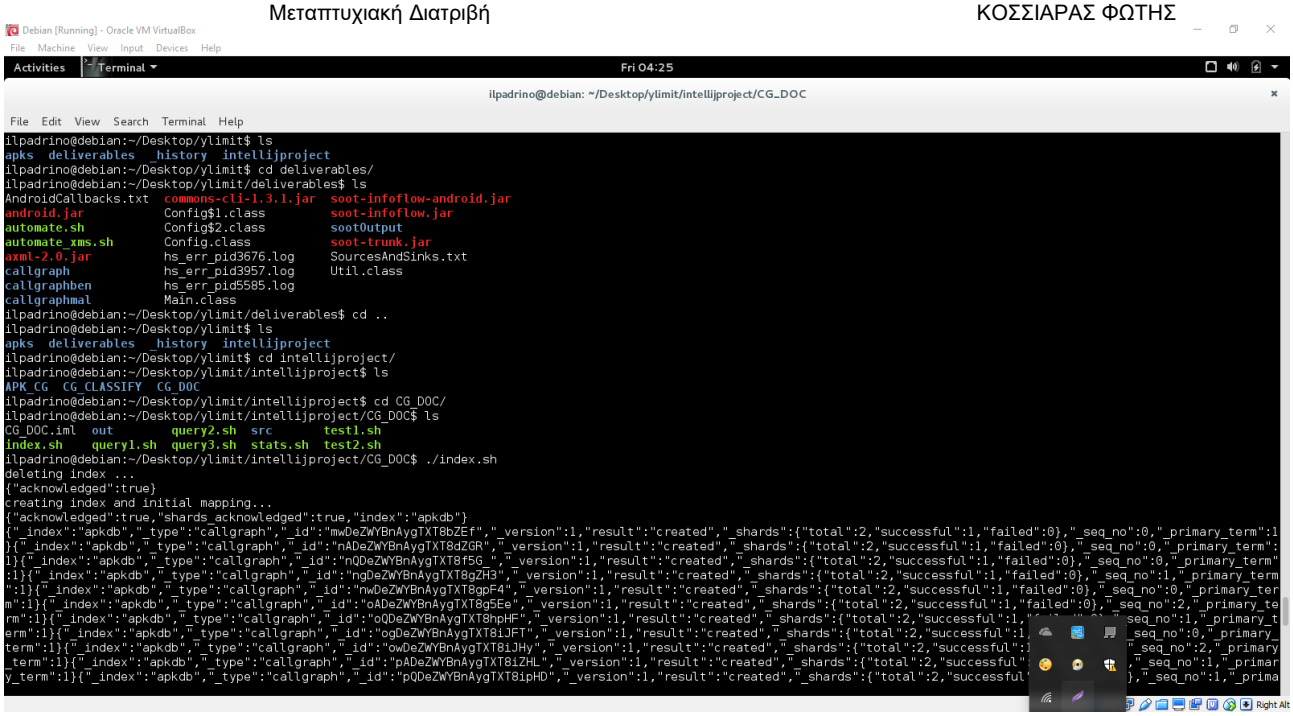
/home/ilpadrino/Desktop/ylimit/deliverables/callgraphmal/



Indexing

Η έξοδος του CG_DOC μας εδωσε το εκτελεσιμο αρχειο index.sh, οπου με την εκτελεση του θα μας κανει τη ευρητηριοποιση

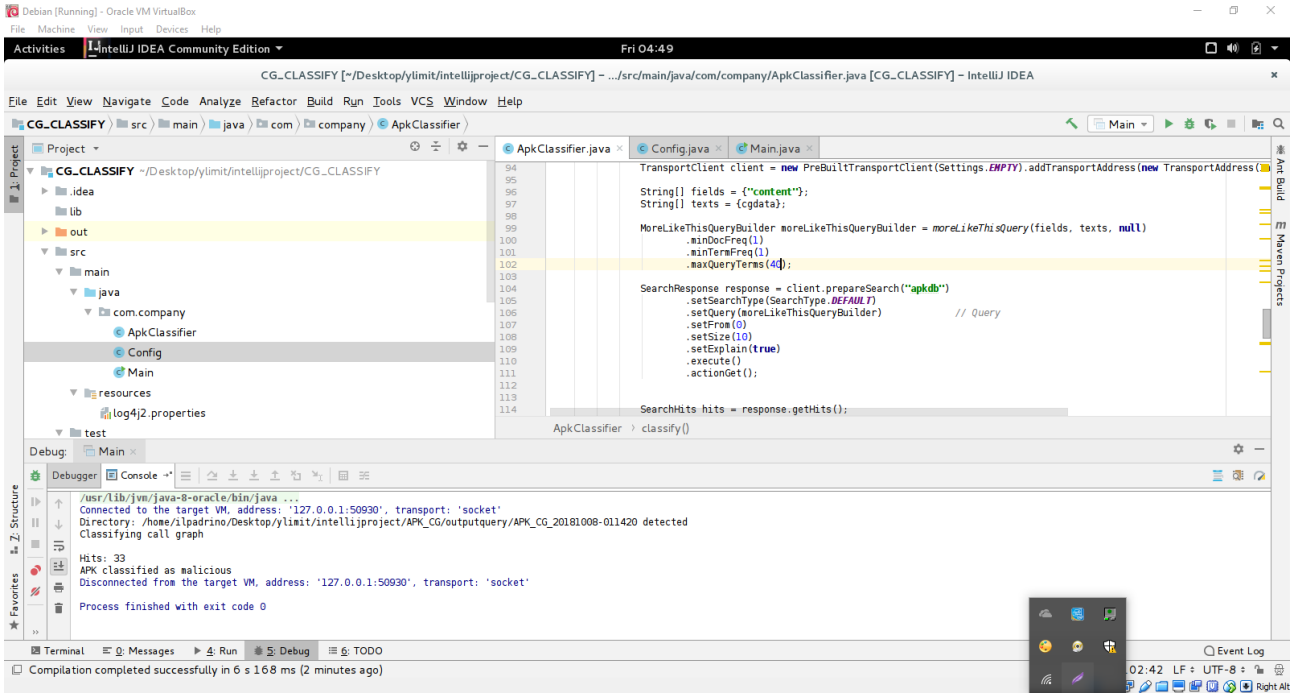
./index.sh



Classification

Δίνοντας σαν είσοδο στον αλγόριθμο CG_CLASSIFY το μονοπάτι στο οποίο είναι αποθηκευμένο το callgraph του αγνώστου apk, θα μας δωσει ως έξοδο μετα την αναζητηση που θα πραγματοποιήσει στο elastic search.

/home/ilpadrino/Desktop/ylimit/intellijproject/APK_CG/outputquery



Πηγές

ΣΎΝΔΕΣΜΟΙ ΙΣΤΟΣΕΛΊΔΩΝ

https://file.scirp.org/pdf/JIS_2014040110394271.pdf

https://medium.com/mindorks/static-code-analysis-for-android-using-findbugs-pmd-and-checkstyle-3a2861834c6a

https://www.sciencedirect.com/science/article/abs/pii/S0950584912001012

https://code.tutsplus.com/tutorials/ensure-high-quality-android-code-with-static-analysis-tools--cms-28787

https://github.com/secure-software-engineering/FlowDroid/tree/master/soot-infoflow-android

https://www.exploit-db.com/docs/english/33093-introduction-to-android-malware-analysis.pdf

https://www.rsaconference.com/writable/presentations/file_upload/mbs-r02-how-to-analyze-an-android-bot.pdf

https://www.elastic.co/

https://www.intechopen.com/books/smartphones-from-an-applied-research-perspective/malware-analysis-and-detection-on-android-the-big-challenge

ΒΙΒΛΙΟΓΡΑΦΊΑ

http://www.dunkelheit.com.br/android/forense/curso/curso/%5BKen_Dunham%5D_Android_Malware_and_Analysis(BookZZ.org).pdf

https://el.wikipedia.org/wiki/Android

http://www.allaboutandroid.gr/?p=6362

http://cs.au.dk/~mis/soot.pdf

https://towardsdatascience.com/getting-started-with-elasticsearch-in-python-c3598e718380