ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

Μάθημα: Ιδιωτικότητα στο Διαδίκτυο

Επιβλέπων καθηγητής: Κύριος Στέφανος Γκρίτζαλης

Θέμα Εργασίας:

Spyware and Privacy

Φοιτητές:

Στέφανος Δαρδαμάνης Ε20038

Αντώνης Παπακωνσταντίνου Ε20124

Περιεχόμενα

Περίληψη

Η παρούσα εργασία ασχολείται με τα ζητήματα προστασίας της ιδιωτικής ζωής που σχετίζονται με το λογισμικό υπολογιστών που έχει γίνει γνωστό ως λογισμικό κατασκοπείας (spyware). Αποτελεί τον πιο κοινό κίνδυνο στο διαδίκτυο για εταιρείες και μεμονωμένους χρήστες όσον αφορά την Ιδιωτικότητα τους. Οι ανησυχίες για την προστασία της ιδιωτικής ζωής έχουν αρχίσει να συζητούνται στο διαδίκτυο και στα εμπορικά μέσα ενημέρωσης. Θα εξετάσουμε βασικές έννοιες του κατασκοπευτικού λογισμικού , διάφορους τύπους αυτού, τις μεθόδους διάδοσής του , τις επιπτώσεις του στην ιδιωτικότητα του ατόμου, καθώς και τις συνέπειές του στην κοινωνία. Επιπλέον , θα παραθέσουμε διάφορα παραδείγματα εφαρμογής του κατασκοπευτικού λογισμικού από τη συλλογή δεδομένων επιστημονικών ερευνών και πειραματικών μελετών.

Κεφάλαιο 1: Εισαγωγή

Στην σύγχρονη εποχή της ευρείας τεχνολογικής επανάστασης και της συνεχούς εξέλιξης τεχνολογικών εφαρμογών, έχουμε γίνει μάρτυρες μιας αναπτυσσόμενης εποχής που χαρακτηρίζεται από αυξημένη παραγωγικότητα, βελτιωμένη επικοινωνία και προηγμένες δυνατότητες πληροφόρησης. Η τεχνολογία έχει επιτρέψει την ανάπτυξη νέων επιχειρηματικών μοντέλων, την επιτάχυνση της επιστημονικής έρευνας και την ενίσχυση της παγκόσμιας συνεργασίας.

Ωστόσο, παρά τα θετικά αυτής της εποχής, υπάρχουν και κινδύνοι που ελλοχεύουν δρώντας με απώτερο σκοπό το κέρδος. Μερικοί από τους κινδύνους αυτούς είναι διάφοροι ιοί (malwares) όπου δρουν στον υπολογιστή του θύματος με σκοπό την κλοπή προσωπικών δεδομένων (όπως κωδικοί πρόσβασης ebanking). Ένας από τους πιο κοινούς κινδύνους για τα προσωπικά δεδομένα και την παραβίαση της ιδιωτικότητας είναι τα διάφορα κατασκοπευτικά λογισμικά (spyware).

Το κατασκοπευτικό λογισμικό (spyware), είναι ένας τύπος λογισμικού που παρακολουθεί τη χρήση του υπολογιστή χωρίς τη συναίνεση του χρήστη, Αυτό αποτελεί μια σημαντική πρόκληση για την κοινωνία μας, καθώς η προστασία της ιδιωτικής ζωής είναι ζωτικής σημασίας για τη δημοκρατία και την ελευθερία του ατόμου.

Το κατασκοπευτικό λογισμικό αποτελεί έναν τύπο λογισμικού που εγκαθίσταται στον υπολογιστή του θύματος χωρίς την γνώση ή την συναίνεση αυτού. Μετά την διείσδυση στην προσωπική συσκευή, με άγνωστες διεργασίες που περιέχει, παρακολουθεί τη δραστηριότητα του κεντρικού υπολογιστή του θύματος, έχει την δυνατότητα να κλέψει τα ευαίσθητα προσωπικά δεδομένα αλλά και δεδομένα περιήγησης του διαδικτύου, και να στείλει τις πληροφορίες σε έναν υπεύθυνο κατασκοπείας με σκοπό να τις πουλήσει σε τρίτους, με το ανάλογο αντίτιμο. Ως εκ τούτου, είναι συχνά δύσκολο, ακόμη και για έμπειρους χρήστες, να διακρίνουν εάν σε κάθε τους κίνηση στο διαδίκτυο υπάρχει πρόθεση κατασκοπείας.

Είναι, λοιπόν, απαραίτητο σε αρχικό στάδιο να μελετήσουμε τι είδους κίνδυνος είναι αυτός , από τι αποτελείται, ποια είναι τα είδη κατασκοπευτικού λογισμικού που υπάρχουν, και αφού αναπτύξουμε μία σφαιρική άποψη επί του κινδύνου να αναπτύξουμε στρατηγικές και μέτρα για την αντιμετώπιση αυτής της απειλής, προκειμένου να διασφαλίσουμε την ασφάλεια και την ιδιωτικότητα των πολιτών στον ψηφιακό κόσμο.

Κεφάλαιο 2: Ανάλυση των εννοιών

Η Ιδιωτικότητα αποτελεί μία θεμελιώδη αρχή στην κοινωνία μας, η οποία συχνά υποβαθμίζεται από διάφορες μορφές παρακολούθησης , μέσω του κατασκοπευτικού λογισμικού. Τέτοιου είδους λογισμικά αποτελούν μία από τις πιο επικίνδυνες πρακτικές για την παραβίαση της ιδιωτικότητας κάποιου ατόμου . Για να κατανοήσουμε πλήρως τη σημασία της ιδιωτικότητας και τον κίνδυνο που αποτελεί το κατασκοπευτικό λογισμικό, πρέπει να εξετάσουμε προσεκτικά τις εννοιολογικές και λειτουργικές πτυχές και των δύο.

Η Ιδιωτικότητα αναφέρεται στο δικαίωμα και την ικανότητα ενός ατόμου να διαχειρίζεται τις πληροφορίες που το αφορούν, καθώς και τον τρόπο με τον οποίο αυτές οι πληροφορίες διανέμονται και χρησιμοποιούνται από άλλους. Είναι ένα θεμελιώδες ανθρώπινο δικαίωμα που εξασφαλίζει την ατομική ελευθερία και αυτοδιάθεση. Η Ιδιωτικότητα περιλαμβάνει την προστασία των προσωπικών δεδομένων και την αποτροπή αποκάλυψής τους χωρίς τη συναίνεση του εκάστοτε ατόμου.

Η προστασία της ιδιωτικότητας είναι ζωτικής σημασίας για την ελευθερία και την αυτονομία των ατόμων στην ψηφιακή εποχή. Η απώλεια της ιδιωτικότητας μπορεί να οδηγήσει σε καταστάσεις όπου οι ατομικές ελευθερίες περιορίζονται και η αυτονομία υπονομεύεται. Μέσα από την προστασία της ιδιωτικότητας διασφαλίζουμε τη δυνατότητα των ατόμων να διατηρούν έναν βαθμό ανωνυμίας και ελευθερίας στον ψηφιακό κόσμο. Ωστόσο, η παραβίαση της μέσω του κατασκοπευτικού λογισμικού μπορεί να οδηγήσει σε σοβαρές συνέπειες για τους χρήστες αλλά και την κοινωνία συνολικά.

Αρχικά, η απώλεια της ιδιωτικότητας μπορεί να οδηγήσει σε μια κατάσταση όπου οι ατομικές ελευθερίες περιορίζονται σημαντικά. Όταν οι προσωπικές πληροφορίες εκτίθενται σε κακόβουλους επιτιθέμενους ανθρώπους, τα θύματα μπορεί να υποχρεωθούν να περιορίσουν την πρόσβαση στο διαδίκτυο ή να αποφύγουν τη χρήση ψηφιακών υπηρεσιών εντελώς, περιορίζοντας έτσι τις δυνατότητές τους για επικοινωνία, πληροφόρηση και δραστηριότητες στο διαδίκτυο. Στην εποχή όπου τα πάντα γίνονται μέσα από το διαδίκτυο ξέρουμε πόσο μπορεί να κοστίσει αυτό. Επίσης, η απώλεια ιδιωτικότητας μπορεί να υπονομεύσει την αυτονομία των ατόμων. Όταν οι προσωπικές τους πληροφορίες χρησιμοποιούνται χωρίς την άδειά τους για σκοπούς όπως η διαφήμιση, η εκπαίδευση συστημάτων AI , η παρακολούθηση ή η εκμετάλλευση, οι άνθρωποι χάνουν τον έλεγχο επί της δικής τους πληροφορίας και της διαδικτυακής τους παρουσίας. Αυτό μπορεί να οδηγήσει σε αίσθημα ανασφάλειας και απώλειας εμπιστοσύνης στον ψηφιακό κόσμο. Τέλος, η απώλεια της ιδιωτικότητας μπορεί να έχει ευρύτερες κοινωνικές συνέπειες. Όταν οι πληροφορίες των ατόμων εκτίθενται σε κακόβουλους τρίτους, αυτό μπορεί να οδηγήσει σε εκβιασμούς, παραβιάσεις της ατομικής ασφάλειας και αύξηση του εγκλήματος διαδικτυακής απάτης και κακοποίησης.

Συμπερασματικά, η προστασία της ιδιωτικότητας είναι κρίσιμη για τη διασφάλιση μιας ελεύθερης και αυτόνομης ψηφιακής εποχής, όπου οι χρήστες μπορούν να απολαμβάνουν τα οφέλη της τεχνολογίας χωρίς να υποκύπτουν σε κακόβουλες πρακτικές ή παρεμβάσεις στην προσωπική τους ζωή.

Από την άλλη πλευρά , το κατασκοπευτικό λογισμικό είναι ένα είδος λογισμικού που εγκαθίσταται στον υπολογιστή του θύματος χωρίς τη συναίνεση ή την γνώση αυτού. Στη συνέχεια, παρακολουθεί τη δραστηριότητα του υπολογιστή, κλέβει ευαίσθητα προσωπικά

δεδομένα και τα στέλνει σε έναν υπεύθυνο κατασκοπείας (κατά πάσα πιθανότητα τον επιτιθέμενο) με σκοπό την πώλησή τους ή τη χρήση τους για επιθέσεις και κακόβουλες δραστηριότητες.

Η βασική ιδέα του κατασκοπευτικού λογισμικού είναι να δίνει στους επιτιθέμενους πρόσβαση σε ευαίσθητες πληροφορίες και δεδομένα του θύματος, όπως κωδικούς πρόσβασης, προσωπικά μηνύματα, ιστορικό πλοήγησης στο διαδίκτυο και άλλα προσωπικά αρχεία. Αυτές οι πληροφορίες μπορούν στη συνέχεια να χρησιμοποιηθούν για κακόβουλους σκοπούς, όπως η κλοπή ταυτότητας, η εξαπάτηση, η αποστολή ανεπιθύμητων διαφημίσεων ή ακόμη και η πώλησή τους σε τρίτους.

Το κατασκοπευτικό λογισμικό λειτουργεί συχνά σαν εργαλείο για κυβερνοεπιθέσεις και διαδικτυακά εγκλήματα. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τις πληροφορίες που συλλέγονται από το κατασκοπευτικό λογισμικό για να πραγματοποιήσουν εξαπατήσεις, να προβούν σε απάτες ή ακόμα και να εκβιάσουν τα θύματά τους.

Το κατασκοπευτικό λογισμικό αποτελεί σοβαρή απειλή για την ιδιωτικότητα και την ασφάλεια των ατόμων. Με την αόρατη παρακολούθηση των δραστηριοτήτων τους, οι χρήστες εκτίθενται σε εκμετάλλευση, κλοπή ταυτότητας και άλλες μορφές κυβερνοεπιθέσεων. Όλο αυτό μπορεί να οδηγήσει σε σοβαρές παραβιάσεις της ατομικής ζωής και της αυτονομίας τους

Μέσα από την ανάλυση που προηγήθηκε στο κεφάλαιο αυτό, γίνεται φανερό πόσο σημαντικό είναι να προστατεύουμε την Ιδιωτικότητα και πώς η απώλειά της μπορεί να επηρεάσει την καθημερινότητά μας και την κοινωνία συνολικά. Η ιδιωτικότητα αποτελεί κεντρικό θέμα στην ψηφιακή εποχή, ενώ το κατασκοπευτικό λογισμικό αποτελεί μία από τις πιο επικίνδυνες απειλές για αυτήν. Είναι σαφές ότι η προστασία της ιδιωτικότητας απαιτεί προληπτικά μέτρα και ευαισθησία από τους χρήστες και τους διαχειριστές συστημάτων πληροφορικής. Μέσω της ενημέρωσης και της πραγματοποίησης βέλτιστων πρακτικών, μπορούμε να προστατεύσουμε την Ιδιωτικότητα μας και να διατηρήσουμε την ασφάλεια μας στο διαδίκτυο.

Κεφάλαιο 3: Παραδείγματα κατασκοπευτικού λογισμικού

3.1 Λογισμικό Παρακολούθησης δεδομένων εισαγωγής (Key-loggers)

Ο συγκεκριμένος τρόπος παρακολούθησης αποτελεί μια δύσκολη ανιχνεύσιμη τεχνική που έχει δυο τρόπους διεκπεραίωσης:

1. **Με λογισμικό (Software Key-logger):** Μπορεί να εκχωρηθεί με πρόθεση από κάποιο επιτιθέμενο, ή να εγκατασταθεί με ή χωρίς θέληση από κάποιο χρήστη.
2. **Με υλισμικο (Hardware Key-logger):** Είναι πανομοιότυπο με ένα φορητό δισκάκι (USB Flash Drive), παριστάνοντας μία κοινότυπη σύνδεση μεταξύ υπολογιστή και πληκτρολογίου.

Ως βασική λειτουργία έχει να καταγράφει τα δεδομένα που εισάγει ο στόχος δια μέσω του πληκτρολογίου του, χωρίς όμως να είναι αντιληπτή η ύπαρξη αυτού του λογισμικού. Γνωρίζοντας ότι οι περισσότερες πληροφορίες εισάγονται δια μέσω του πληκτρολογίου κατά κύριο λόγο αποτελεί ένα αποτελεσματικό, χρήσιμο μέσω κατασκοπίας, αφήνοντας λιγοστά περιθώρια στον στόχο να διαφύγει. Έχοντας ως αποτέλεσμα ένας χρήστης κατά την εισαγωγή κρίσιμων πληροφοριών, όπως είναι τα δεδομένα πιστωτικών καρτών ή και τα στοιχεία σύνδεσης σε διάφορες πλατφόρμες, αυτές να καταγράφονται σε ένα κρυπτογραφημένο αρχείο (Log file), που αυτό έπειτα στέλνεται στον επιτιθέμενο. Να σημειωθεί ότι το λογισμικό αυτό δεν είναι απαραίτητα παράνομο ή χρησιμοποιήσιμο για αποκλειστικά βλαβερές και υπονομευνομευτικές ενεργειες. Διότι πέρα απο την παράνομη κατασκοπία μπορεί να χρησιμοποιηθεί για παρακολουθήσεις στόχων που είναι επικίνδυνοι για την εθνική ασφάλεια, για την εποπτεία υπολογιστών που χρησιμοποιούν άτομα μικρότερης ηλικίας αλλά και υπαλλήλων (με την απαραίτητη συναίνεση πάντα) ή ακόμη για την διασφάλιση του αδιάβλητου μίας εξέτασης.

3.2 Λογισμικό Διαφημίσεων (Adware)

Το ολόκληρο όνομά του είναι λογισμικό υποστήριξης διαφημίσεων (Advertising Supported Software). Στην οικογένεια αυτού εντάσσονται όλα τα είδη λογισμικού που εμφανίζουν διαφημιστικό υλικό σε έναν υπολογιστή. Το εν λόγω λογισμικό εμφανίζει μη επιθυμητές και αρκετές φορές ενοχλητικές διαφημίσεις σε μορφή αναδυόμενων παραθύρων (pop-ups) στην οθόνη του υπολογιστή ή του κινητού. Οι τρόποι που μπορεί να 'μολυνθεί' μια συσκευή από αυτό το λογισμικό είναι:

1. Με την εγκατάσταση δωρεάν λογισμικού ή εφαρμογής που δεν είναι εμφανές ότι διαθέτει κάποιο λογισμικό διαφημίσεων.
2. Με την εύρεση από έναν επιτηθέμενο ενός κενού ασφαλείας στο λειτουργικό του υπολογιστή, μπορεί να εγκαταστήσει διάφορους υιούς που μπορεί ένας εκ των οποίων να είναι λογισμικό διαφημίσεων. Ο τρόπος που λαμβάνουν χρήματα οι δημιουργοί αυτών είναι είτε με το πάτημα της διαφήμισης, είτε με την απλή προβολή της διαφήμισης, είτε με κάθε εγκατάσταση από το λογισμικό που παρουσιάζει τη διαφήμιση. Ορισμένες εκδόσεις μπορεί να δυσκολέψουν τη χρήση της συσκευής από τον χρήστη, για παράδειγμα κάνοντας την πιο αργή, και αυτά τα σημάδια δυσκολίας αποτελούν στοιχεία ώστε το θύμα να αντιληφθεί την μόλυνση. Εκτός αυτού μπορεί να φέρει τον χρήστη σε επαφή με ιστοσελίδες αλλά και

περιεχόμενο για ενήλικους, που πλησίον φορές είναι ανεπιθύμητο. Επιπλέον εάν η διαφήμιση είναι κακόβουλη, σε περίπτωση που ο χρήστης την πατήσει, μπορεί να μεταφερθεί σε κάποια επιβλαβή ιστοσελίδα ή να εγκαταστήσει αυτόματα κακόβουλο λογισμικό που θα οδηγήσει στην κλοπή προσωπικών δεδομένων.

3.3 Κατασκοπευτικός Δούρειος Ίππος (Spy Trojans)

Ο Δούρειος Ίππος αποτελεί ένα λογισμικό που εγκαθίσταται από τον χρήστη σαν έγκυρο, εξού και αυτή η ονομασία, οπότε ο τρόπος εγκατάστασης βασίζεται στο επιτυχές καμουφλάρισμα ενός κακόβουλου λογισμικού. Σκοπός αυτού είναι να βλάψει με αρκετούς τρόπους τον εκάστοτε υπολογιστή και τον ιδιοκτήτη αυτού, ένας εκ των οποίων είναι η κλοπή δεδομένων. Μετά από την εγκατάσταση μπορεί να δεσμεύσει διάφορα αρχεία, να αποθηκεύσει μια στιγμιαία καταγραφή οθόνης (screenshot), να υποκλέψει συνθηματικά συνδέσεων σε εφαρμογές και άλλα πολλά κατασκοπευτικά ενέργειες. Υπάρχει μια πιο εξειδικευμένη εκδοχή αυτού του λογισμικού που ονομάζεται Τραπεζικοί Δούρειοι Ίπποι (Banking Trojans) που έχει σαν στόχο οργανισμούς που έχουν σχέση με την οικονομία, όπως τράπεζες. Ο τρόπος που ενεργεί είναι αλλάζοντας ιστοσελίδες σε ένα διαδικτυακό ιστοχώρο τράπεζας, κάνοντας συναλλαγές με σκοπό να επωφεληθεί ο επιτιθέμενος αλλά και αλλάζοντας τιμές σε διάφορες συναλλαγές. Ορισμένες εκδοχές μπορεί να λειτουργούν και σαν Παρακολουθητές Δεδομένων Εισαγωγής (Key-loggers όπως είδαμε στο πρώτο είδος) καταγράφοντας δεδομένα που εισάγονται δια μέσω πληκτρολογίου ή και ακόμη κλοπή αρχείων με ευαίσθητα δεδομένα.

3.4 Λογισμικό Παρεμβολών στον Περιηγητή (Browser Hijackers)

Το συγκεκριμένο είδος είναι πρακτικά το λογισμικό που δρα σε διαδικτυακό ιστοχώρο, αλλάζοντας τις ρυθμίσεις αλλά και τη δραστηριότητα αυτού χωρίς τη συγκατάθεση του χρήστη. Αυτό έχει ως αποτέλεσμα να δρομολογεί την κίνηση των δεδομένων αλλά και του ίδιου του χρήστη σε κακόβουλες ιστοσελίδες. Αυτό μπορεί να αποτελέσει μέσο παραπλάνησης (Social Engineering), κάνοντας τον χρήστη να νομίζει ότι βρίσκεται σε έγκυρη ιστοσελίδα και να δώσει τα στοιχεία σύνδεσης. Έτσι ο επιτιθέμενος θα έχει τα στοιχεία για παράδειγμα της τράπεζας του χρήστη (e-banking credentials). Σε άλλη περίπτωση μπορεί να κατεβάσει/εγκαταστήσει άθελα του λογισμικό κατασκοπείας όπως για παράδειγμα έναν Παρακολουθητή δεδομένων εισαγωγής ή κάποιο Λογισμικό Διαφημίσεων. Επιπλέον είναι σύνηθες να είναι ένα απλό πρόγραμμα, που έχει τοποθετηθεί συνειδητά από την εκάστοτε εταιρεία. Ως σκοπό έχει να ελέγχει και να καταγράφει την κίνηση του χρήστη χωρίς τη δική του συγκατάθεση. Δεν αποτελεί ιδίας βαρύτητας επίπτωση προς τον χρήστη όπως στις άλλες περιπτώσεις, αλλά συνεχίζει να αποτελεί παραβίαση της ιδιωτικότητας του, διαμέσω της κατασκοπείας και καταγραφής των κινήσεών του.

3.5 Λογισμικό Διείσδυσης (Rootkit)

Αποτελεί ένα λογισμικό κατασκευασμένο με απώτερο σκοπό να δίνει πρόσβαση του επιτιθέμενου στον υπολογιστή του στόχου, χωρίς να γίνονται αντιληπτοί. Έτσι ο επιτιθέμενος δρα αθόρυβα παρακολουθώντας τις κινήσεις του χρήστη αλλά και

δεσμεύοντας δεδομένα. Ανάλογα με τον τρόπο που εγκαθίστανται και εκμεταλλεύονται το σύστημα χωρίζονται σε 5 κατηγορίες:

1. **Λογισμικό Διείσδυσης Υλικολογισμικού (Firmware Rootkits):** Έχει ως στόχο τα συστήματα εισόδου/εξόδου και τον σκληρό δίσκο του υπολογιστή οπότε μπορεί να έχει πρόσβαση σε κρίσιμα δεδομένα.

2. **Λογισμικό Δεισδυσης του Λογισμικού Εκκίνησης (Bootloader Rootkits):** Έχει ως στόχο το πρόγραμμα εκκίνησης του υπολογιστή, αντικαθιστώντας αυτό με ένα παραλλαγμένο έχοντας ως αποτέλεσμα να υπάρχουν και προγράμματα κατασκοπείας κινήσεων.

3. **Λογισμικό Διείσδυσης Μνήμης (Memory Rootkits):** Αυτή η κατηγορία έχει σχέση κυρίως με την προσβολή της μνήμης τυχαίας προσπέλασης (Random Access Memory-RAM), θέλοντας να μειώσει την απόδοση του μηχανήματος.

4. **Λογισμικό Διείσδυσης Εφαρμογής (Application Rootkits)**: Σε αυτή την εκδοχή το λογισμικό αλλάζει εφαρμογές στον υπολογιστή αντικαθιστώντας αυτές με κακόβουλες εφαρμογές. Αυτό μπορεί να οδηγήσει σε κλοπή κωδικών (Ο χρήστης νομίζει ότι είναι έγκυρη εφαρμογή), αλλά και σε καταγραφή κινήσεων αλλά δεδομένων εισόδου.

5. **Λογισμικό Διείσδυσης πυρήνα (Kernel Mode Rootkits)**: Αυτό το λογισμικό έχει ως στόχο το λειτουργικό σύστημα του υπολογιστή, με σκοπό να πάρει πρόσβαση στο μηχάνημα και να κλέψει δεδομένα αλλά και να αλλάξει τον τρόπο λειτουργίας του.

Σε γενικό πλαίσιο αξίζει επίσης να σημειωθεί ότι με την εκτέλεση κατανεμημένης επίθεσης απόρριψης υπηρεσιών (Distributed Denial Of Service Attack-DDOS) από αυτού του είδους τα λογισμικά, απενεργοποιούνται οι υπηρεσίες ασφαλείας, οπότε μπορούν να κλαπούν ευαίσθητα δεδομένα.

3.6 Παρακολούθηση με χρήση αρχείων δεδομένων περιήγησης (Cookie Trackers)

Τα αρχεία δεδομένων περιήγησης, γνωστά και ως "cookies", αποτελούν μια θεμελιώδη τεχνική για την αποθήκευση δεδομένων από τους ιστότοπους ώστε να σε θυμούνται. Σε αποθηκεύονται γεωγραφικά δεδομένα, προηγούμενες αναζητήσεις, προτιμήσεις και άλλες χρήσιμες πληροφορίες, δημιουργώντας ένα προφίλ χρήστη για να κάνουν την εμπειρία του καλύτερη. Επιπλέον, χρησιμοποιούνται για σκοπούς μάρκετινγκ, θέλοντας να προωθήσουν τα κατάλληλα προϊόντα. Όλα αυτά προϋποθέτουν τη συγκατάθεση του χρήστη, αλλιώς αποτελεί παραβίαση ιδιωτικότητας. Αυτός είναι ο σκοπός πολλών "cookies" που συλλέγουν γεωγραφικά δεδομένα αλλά και κινήσεις περιήγησης χωρίς να έχουν λάβει την απαραίτητη συγκατάθεση. Οπότε σε αυτή την περίπτωση μπορούμε να πούμε ότι ο χρήστης είναι θύμα κατασκοπείας. Παράλληλα, σε αντίθεση με τα προηγούμενα είδη, είναι το λιγότερο ακίνδυνο καθώς δεν είναι δύσκολη η διαγραφή και η απενεργοποίησή τους, αλλά επίσης στις περισσότερες περιπτώσεις δεν υποκλέπτουν πολύ σημαντικά δεδομένα ούτε βλάπτουν τον προσωπικό υπολογιστή του καθενός.

3.7 Διαδικτυακά Φανάρια (Web Beacon)

Τα διαδικτυακά φανάρια είναι πρακτικά αρχεία που καταγράφουν σε ένα συγκεκριμένο ιστοχώρο τη δραστηριότητα του χρήστη. Ονομάζονται επίσης και εικονοστοιχεία παρακολούθησης (Tracking pixels), εικονοστοιχεία κατασκοπείας (Spy pixels) και διαδικτυακό "σκαθάρι" (Web bug). Συνήθως είναι ένα εικονοστοιχείο μη ορατό από τον χρήστη λόγω μεγέθους, με εσωτερικό προγραμματισμό που του θέτει ως σκοπό την καταγραφή της επισκεψιμότητας του ιστοχώρου. Όπως και στα "cookies", τίθεται κυρίως ζήτημα παραβίασης ιδιωτικότητας μέσω της παρακολούθησης.

3.8 Κατασκοπευτικό Λογισμικό Κινητού (Mobile Spyware)

Το συγκεκριμένο λογισμικό κρύβεται στο παρασκήνιο του κινητού τηλεφώνου και με ένα σύνολο εργαλείων κατασκοπείας καταγράφει και κλέβει πληροφορίες όπως είναι εισερχόμενα/εξερχόμενα μηνύματα κινητού (SMS) αλλά και ηλεκτρονικού ταχυδρομείου (Email), επαφές, φωτογραφίες, αρχεία και γενικά οποιαδήποτε πληροφορία χρήσιμη μπορεί να αποσπάσει. Πέραν αυτών, μπορεί να ενεργοποιήσει οποιαδήποτε εφαρμογή του κινητού (κάμερα, μικρόφωνο, κλήσεις) αλλά και το σύστημα εντοπισμού (Global Positioning System - GPS) γνωστοποιώντας έτσι όχι τη θέση του θύματος αλλά και τις καθημερινές μεταφορές ρουτίνας. Η εγκατάστασή του είναι ανάλογα με το κατασκοπευτικό λογισμικό που θα χρησιμοποιηθεί, καθώς πολλά χρειάζονται τον "ανθρώπινο παράγοντα" για να εγκατασταθούν, δια μέσω κάποιου συνδέσμου, κάποιου μηνύματος ή κάποιου συνημμένου ηλεκτρονικού ταχυδρομείου, ενώ άλλα εγκαθίστανται χωρίς να κάνει κάποια υπονομευτική ενέργεια ο χρήστης. Είναι από τα πιο επικίνδυνα κατασκοπευτικά λογισμικά, καθώς στη σύγχρονη εποχή το κινητό αποτελεί το πιο συχνό μέσο επικοινωνίας μας αλλά και γενικής χρήσης, άρα η πλήρης εποπτεία του οδηγεί σε τεράστια παραβίαση της ιδιωτικότητας.

3.9 Λογισμικό Ψηφιακής Παρακολούθησης (Stalkware, Spouseware)

Είναι ένα προϊόν που προωθείται σαν νόμιμο αντικλεπτικό λογισμικό αλλά και για χρήση γονικής εποπτείας κατά των ανηλίκων, αλλά διαφέρει από την πραγματικότητα. Αρχικά εγκαθίσταται χωρίς την συγκατάθεση του χρήστη της και δεν υπάρχει στην λίστα εφαρμογών της συσκευής, κάνοντας έτσι το λογισμικό δύσκολο προς εντοπισμό. Οι λειτουργίες αυτού είναι να καταγράφει μηνύματα που στέλνονται ή λαμβάνονται, το ιστορικό κλήσεων, την λίστα επαφών αλλά και να διαβάζει δεδομένα εφαρμογών κοινωνικής δικτύωσης (Instagram, Facebook, Viber κ.α.). Επιπλέον δίνεται το δικαίωμα την προβολής εικόνων και βίντεο της μνήμης, της καταγραφής της γεωγραφικής θέσης αλλά και την διενέργεια φωτογράφισης δια μέσου της μπροστινής κάμερας ή απλά της στιγμιαίας καταγραφής της οθόνης του κινητού. Οπότε γίνεται αντιληπτό ότι παραβιάζεται κατά κόρων η ιδιωτικότητα και η προσωπική ζωή του ατόμου, κάνοντας την αντικείμενο ενός τρίτου.

Κεφάλαιο 4: Ο Κίνδυνος των Pegasus και Predator Spyware

Δύο από τα πιο ανησυχητικά εργαλεία που έχουν προκύψει είναι τα Pegasus και Predator spyware (Κατασκοπευτικά Λογισμικά). Αυτά τα εργαλεία, που αρχικά θεωρούνταν αποκλειστικά ως μέσα για την επιτήρηση εγκληματικών στοιχείων ή κρατική παρακολούθηση, έχουν επεκταθεί στον ψηφιακό κόσμο με ανησυχητικό τρόπο.

Το κατασκοπευτικό λογισμικό Pegasus είναι το πιο προηγμένο και εξελιγμένο κακόβουλο λογισμικό που υπάρχει. Είναι πολύ επικίνδυνο επειδή η αρχή του είναι η " Zero-day Vulnerability" (Ευπάθεια μηδενικής ημέρας). Οι μηδενικές ευπάθειες είναι αυτές οι αδυναμίες για τις οποίες δεν υπάρχει ενημέρωση επιδιόρθωσης ή οι χρήστες δεν τις έχουν ανακαλύψει ακόμα. Είναι ένα διαφορετικό είδος κακόβουλου λογισμικού που κατασκοπεύει τις ενέργειες που κάνει το θύμα μέσω διαφόρων κινητών συσκευών είτε Android είτε iPhone. Ο επιτιθέμενος μπορεί να έχει πλήρη πρόσβαση στη συσκευή και να κάνει διάφορα πράγματα όπως:

1. **Ανάγνωση μηνυμάτων**
2. **Έλεγχος φωτογραφιών**
3. **Παρακολούθηση βίντεο**
4. **Κλήσεις τηλεφώνου**
5. **Πρόσβαση στα αρχεία κλήσεων**
6. **Καταγραφή τοποθεσιών**
7. **Ενεργοποίηση μικροφώνου και κάμερας**
8. **Πρόσβαση σε διαγραμμένο περιεχόμενο**

Αυτό το συγκεκριμένο κακόβουλο λογισμικό μπαίνει σε μια συσκευή μόνο με μία αναπάντητο κλήση από το WhatsApp. Μια αναπάντητη κλήση είναι αρκετή ώστε το κακόβουλο λογισμικό να κάνει το έργο του. Επίσης, χρησιμοποιεί το iMessage για να μπει στο iPhone, όπως έχει παρατηρηθεί από διάφορες εκθέσεις και διαφορετικές επιθέσεις που έχουν γίνει. Ο χρήστης ενδεχομένως να μην γνωρίζει καθόλου ότι το κακόβουλο λογισμικό Pegasus έχει αναλάβει τον έλεγχο της συσκευής του. Όπως είδαμε νωρίτερα, λειτουργεί με βάση την έννοια της ευπαθείας Zero-day, έτσι ακολουθεί τη μέθοδο Zero-click, που σημαίνει ότι δεν απαιτείται καμία αλληλεπίδραση με τον χρήστη. Θα κάνει τα απαραίτητα πράγματα μόνο του. Επιπλέον, αν ο χρήστης (το θύμα) προσπαθήσει να διαγράψει το μήνυμα που θεωρεί ύποπτο, το κακόβουλο λογισμικό θα παραμείνει εκεί και θα μολύνει το σύστημα /τη συσκευή του. Μόλις το κακόβουλο λογισμικό μπει στη συσκευή του θύματος, μπορεί εύκολα να έχει πρόσβαση σε μηνύματα, κλήσεις, emails, κωδικούς πρόσβασης, επαφές και μπορεί να τα στείλει όλα στον επιτιθέμενο (που σε αυτή την περίπτωση είναι ο διακομιστής της NSO Group). Λέγεται ότι μπορεί ακόμα να δώσει πρόσβαση ρίζας στον τρίτο (root access), πράγμα που σημαίνει ότι ο επιτιθέμενος μπορεί εύκολα να έχει πρόσβαση στο μικρόφωνο και την κάμερα του θύματος.

Οι πιο πρόσφατες εκδόσεις του Pegasus μπορούν να προσθέσουν κακόβουλους κώδικες μόνο με αναπάντητες κλήσεις στη συσκευή του πιθανού στόχου και επιπλέον αυτό το κακόβουλο λογισμικό διαγράφει αμέσως τα αρχεία κλήσεων και δεν αφήνει κανένα ίχνος χάκινγκ, γεγονός που το καθιστά ακόμα πιο διακριτικό και δύσκολα εντοπίσιμο.Από την άλλη πλευρά , το predator , απαιτεί την αλληλεπίδραση από το υποψήφιο θύμα.

Το Predator είναι ένα λογισμικό παρακολούθησης, και μέσω αυτού , ο επιτιθέμενος μπορεί να αποκτήσει πλήρη πρόσβαση στις λειτουργίες του κινητού τηλεφώνου του θύματος , καθώς και σε όλους τους κωδικούς που έχουν αποθηκευτεί σε αυτό. Στόχοι έχουν υπάρξει κατά καιρούς πολιτικοί, δημοσιογράφοι, ακτιβιστές, αλλά και πολίτες που έπεσαν θύματα διαδικτυακών απατών.

Στις περισσότερες των περιπτώσεων, στέλνεται ένα μήνυμα στα κινητά τηλέφωνα των υποψήφιων θυμάτων, το οποίο τους ζητά να μεταβούν σε έναν συγκεκριμένο ιστότοπο**.** Εάν το θύμα το πατήσει, τότε το Predator αποκτά πλήρη πρόσβαση στο smartphone (αρχεία, εφαρμογές, κωδικούς).

Κεφάλαιο 5: Οφέλη από την χρήση του κατασκοπευτικού λογισμικού

Ο όρος κατασκοπεία στο μεγαλύτερος μέρος του πληθυσμού είναι μια διαδικασία που δεν εντάσσεται στις ενέργειες που έχουν καλόβουλο και νόμιμο πλαίσιο. Παρόλα αυτά είναι γεγονός ότι η κατασκοπία υπό την μορφή παρακολούθησης μπορεί να χρησιμοποιηθεί με νόμιμο και καλόβουλο τρόπο, χωρίς να παραβιάζει την Ιδιωτικότητα των ατόμων και με επίγνωση, τις περισσότερες φορές. Θα παρουσιαστούν παρακάτω μερικές από τις πιο κοινές περιπτώσεις που χρησιμοποιούνται τέτοιου είδους τεχνικές:

- **Αδιάβλητο εξέτασης:** Οντάς στον 21ο αιώνα της τεχνολογικής ανάπτυξης πολλές από τις εξετάσεις που συμμετέχουν οι πολίτες γίνονται εξ αποστάσεως με την χρήση ηλεκτρονικών μέσων. Σε αυτό το γεγονός επηρέασε και σε μεγάλο βαθμό η πανδημία, που ανάγκασε στην αναλογικά γρήγορη μετάβαση σε αυτού του είδους εξέταση. Οπότε είναι αντιληπτό ότι πολλοί χρησιμοποιούν αθέμιτα μέσα με σκοπό την αντιγραφή και μάλιστα σπαταλάνε παραπάνω χρόνο στην εύρεση ενός τρόπου επιτυχίας πάρα στην μελέτη του αντικειμένου. Αυτή η κατάσταση οδήγησε πολλά ιδρύματα να διεξήγαγαν εξετάσεις να βρουν μια λύση για αυτό και η απάντηση σε αυτό το πρόβλημα θα ήταν η εν γνώση παρακολούθηση. Με αλλά λογία πάντα με την συγκατάθεση των εν λόγω εξεταζόμενων θα μπορούσε να εγκατασταθεί μόνο για το δεδομένο χρονικό διάστημα της εξέτασης λογισμικό που θα ελέγχει τις κινήσεις αυτών. Φυσικά δεν θα έχει πρόσβαση σε κανένα από τα ιδιωτικά αρχεία των χρηστών των συσκευών ούτε θα μπορεί να λειτουργήσει μετά το πέρας των εξετάσεων. Δηλαδή δεν θα πρέπει να ξεπερνά τα όρια της παρακολούθησης για τυχόν αθέμιτη συμπεριφορά, παραβιάζοντας έτσι την Ιδιωτικότητα του εκάστοτε διαγωνιζομένου. Αυτή η παρακολούθηση μπορεί να επιτευχθεί με πολλούς τρόπους όπως είναι η χρήση κάμερας και μικροφώνου για την παρακολούθηση της συμπεριφοράς των εξεταζόμενων χωρίς όμως την καταγραφή ή διαμοιρασμό αυτών. Επιπρόσθετα χρήσιμη θα ήταν η εγκατάσταση λογισμικού που θα έχει περίπου την δομή ενός καταγραφέα εισόδων πληκτρολογίου (key logger) με σκοπό να ελέγχονται οι κινήσεις του χρήστη στον υπολογιστή του και όχι απλά της οθόνης καθώς υπάρχουν δίοδοι για την διαφυγή παρακολούθησης.

- **Επίβλεψη παιδιού (προστατευόμενο μέλος):** Ο μέσος ορός ηλικίας απόκτησης κινητής συσκευής ή γενικά πρόσβασης στο διαδίκτυο μειώνεται με τον καιρό αλλά η κριτική ικανότητα και η εμπειρία των μικρών παιδιών μπορεί να τα θέσει σε κίνδυνο. Οπότε για την επίβλεψη έχουν δημιουργηθεί διαφορά λογισμικά παρακολούθησης που εγκαθίστανται στο κινητό ή στην συσκευή που έχει πρόσβαση στο διαδίκτυο. Δια μέσω αυτών γίνεται η επίβλεψη μηνυμάτων, email, ιστορικού παρακολούθησης, χρονικό διάστημα χρήσης εφαρμογών, οι εφαρμογές που χρησιμοποιούνται, ιστορικό κλήσεων ακόμη και γεωγραφική θέση. Με την ανάγνωση αυτών έρχεται στο μυαλό κατευθείαν ότι παραβιάζεται η ιδιωτικότητα του παιδιού. Σκεπτόμενοι όμως τις νεαρές ηλικίες των παιδιών που ο γονιός έχει πλήρη εποπτεία αλλά κυρίως ευθύνη για την ομαλή ένταξη στην κοινωνία, την ορθή

ανάπτυξη και κυρίως την προστασία του παιδιού από διάφορους κίνδυνους που σχετίζονται με τον διαδικτυακό αλλά και τον πραγματικό κόσμο, μπορούμε να δικαιολογήσουμε την νομιμότητα αυτής της ενέργειας.

- **<u>Έλεγχός εταιρικών συσκευών υπαλλήλων(Employee Surveilance) :</u>** Σε αυτή την περίπτωση κυμαινόμαστε σε ποιο λεπτά σημεία καθώς οι υπάλληλοι είναι ανεξάρτητοι ενήλικες οπότε η πλήρης εποπτεία δεν είναι νόμιμη. Οι νομοί αυτοί εναλλάσσονται από κράτος σε κράτος λόγω της διαφορετικής νομοθεσίας που μπορεί να έχει το συγκεκριμένο καθεστώς. Κατά γενική ομολογία οι εργοδότες έχουν δικαίωμα να παρακολουθούν τις συσκευές που δίνουν στους υπάλληλους τους σαν εταιρικές έως κάποια όρια. Θα πρέπει να είναι εντός των ορίων δέσμευσης και καταγραφής δεδομένων που οριοθετεί η συγκεκριμένη νομοθεσία του κράτους αλλά και το λιγότερο δυνατό που χρειάζεται ώστε να ελέγχεται η δραστηριότητα του υπάλληλου. Οπότε με την χρήση λογισμικού ελέγχεται η συσκευή στο επίπεδο παρακολούθησης που είναι επιτρεπτό. Με αλλά λογία ένας εργοδότης στις εταιρικές συσκευές μπορεί να ελέγχει το ιστορικό πρόσβασης αλλά και άλλες ενέργειες όπως είναι η πρόσβαση και διαγραφή αρχείων από τον υπάλληλο αλλά και απλές αναζητήσεις (Όλα αυτά είναι ανάλογα με το όριο παρακολούθησης από την εκάστοτε νομοθεσία). Οι συγκεκριμένοι έλεγχοι γίνονται πάντα με απώτερο σκοπό να ελέγχεται η παραγωγικότητα και ο τρόπος αξιοποίησης του εργατικού χρόνου από τον υπάλληλο. Επιπλέον για να εξασφαλίζεται η προστασία των δεδομένων που βρίσκονται εντός των εταιρικών συσκευών. Αυτά Φυσικά ο υπάλληλος πρέπει να γνωρίζει ότι παρακολουθείται αν και στις περισσότερες περιπτώσεις είναι λογικό ότι συσκευές αποκλειστικά της εταιρίας με κρίσιμα δεδομένα θα ελέγχονται ώστε να μην υπάρξει διαφυγή των δεδομένων αλλά και κάποια μη αδειοδοτημένη πρόσβαση.

- **<u>Παρακολούθηση για λογούς Εθνικής Ασφάλειας (Spy for national security issues) :</u>** Σε αρκετές περιπτώσεις μπορεί η κανονική κατασκοπία ενός πολίτη να αποτελεί νόμιμη πράξη υπό συγκεκριμένους ορούς. Δηλαδή όταν η εκάστοτε αρχή του κάθε κράτος που είναι υπεύθυνη για αυτές τις αποφάσεις, κρίνει αναγκαία την παρακολούθηση ενός οργανισμού ή ενός πολίτη για την διατήρηση της εθνικής ασφάλειας τότε δικαιούται από τον νομό η εκάστοτε αρχή να ξεκινήσει ενέργειες παρακολούθησης. Το επίπεδο παρακολούθησης συνήθως ορίζεται γύρω από την εποπτεία των ηλεκτρικών συσκευών που αποτελούν μέσω επικοινωνίας με οποιοδήποτε τρόπο (τηλέφωνο ή επικοινωνία δια μέσω διαδικτύου), ελέγχοντας κάθε κίνηση του υπόπτου από απλές αναζητήσεις στο διαδίκτυο έως και μηνύματα και κλήσεις που μπορεί να δέχεται ή να κάνει. Να σημειωθεί ότι συνήθως το λογισμικό για αυτή την κατασκοπία είναι ακριβότερο κατά εάν σημαντικό ποσό από τα κοινά μέσα παρακολούθησης που αναφέραμε προγενέστερα, καθώς αποτελεί εάν εργαλείο με πολλές δυνατότητες που είναι άκρως δύσκολο από έναν απλό πολίτη ακόμη και από έναν ειδικό να εντοπιστεί με ευκολία.

Από αυτά τα γενικά παραδείγματα μπορούμε να συμπεράνουμε την χρησιμότητα που μπορεί να έχει η νόμιμη παρακολούθηση/κατασκοπία συγκεκριμένων ατόμων υπό συγκεκριμένες συνθήκες. Αλλά όπως παρατηρήσαμε και στις 4 γενικές περιπτώσεις πρέπει να τίθενται όρια με γνώμονα τον σκοπό της παρακολούθησης, τον στόχο της

παρακολούθησης αλλά και τα όρια της παρακολούθησης όσον αφορά το εύρος καταγραφής των κινήσεων του στόχου. Με την παραβίαση των νομικών ορίων από αυτές ενέργειες, ο εκτελών της παρακολούθησης/κατασκοπίας θα έρθει αντιμέτωπος με την δικαιοσύνη, για παραβίαση των προσωπικών δεδομένων αλλά και της ιδιωτικότητας των ατόμων με ποινή βάση της νομοθεσίας της εκάστοτε χωράς που θα λάβει μέρος το συμβάν.

Κεφάλαιο 6: Επιπτώσεις από την χρήση του κατασκοπευτικού λογισμικού

Οι δυνατότητες του σύγχρονου λογισμικού κατασκόπευσης επιτρέπουν την παρακολούθηση ατόμων σε μαζική και αυτοματοποιημένη κλίμακα. Οι πρόσφατες τάσεις περιλαμβάνουν την τεχνολογία «μηδενικού κλικ» (zero click) που επιτρέπει τη λήψη του spyware σε μια συσκευή χωρίς να χρειάζεται το θύμα να κάνει κλικ σε έναν σύνδεσμο ή να κατεβάσει κάποια εφαρμογή στη συσκευή του, και στη συνέχεια παρέχει απεριόριστη πρόσβαση στην κάμερα, το μικρόφωνο και άλλα προσωπικά δεδομένα. Αυτό το πρωτοφανές επίπεδο εισβολής έχει ως συνέπεια την παραβίαση κάποιων από των θεμελιωδών ανθρωπίνων δικαιωμάτων, όπως η ελευθερία έκφρασης και η ιδιωτική ζωή.

Επί του παρόντος, υπάρχει μικρή διαφάνεια σχετικά με την ανάπτυξη και απόκτηση αυτών των τεχνολογιών. Έρευνες δείχνουν ότι οι εταιρείες τεχνολογίας που αναπτύσσουν κατασκοπευτικό λογισμικό , είναι εξίσου πιθανό να πουλήσουν αυτό το λογισμικό σε αυταρχικά κράτη και εγκληματίες όσο σε δημοκρατικές κυβερνήσεις. Αυτό αποτελεί ανησυχία, όπως ισχυρίζονται συχνά τα αυταρχικά καθεστώτα, που βλέπουν τους δημοσιογράφους, τους αντιφρονούντες και τους ακτιβιστές των ανθρωπίνων δικαιωμάτων ως εγκληματίες ή ως απειλή για την εθνική ασφάλεια, δικαιολογώντας την υποταγή τους σε παρεμβατική επιτήρηση. Όταν οι ομάδες της κοινωνίας των πολιτών είναι στόχος και εκφοβίζονται από spyware, μειώνεται η ικανότητά τους να απαιτήσουν από τις κυβερνήσεις να λογοδοτήσουν και να εξετάσουν περιπτώσεις διαφθοράς, ενώ μπορεί να μειώσει την πολιτική συμμετοχή και να υπονομεύσει τη δημοκρατία.

Η χρήση κατασκοπευτικού λογισμικού έχει σημαντικές επιπτώσεις τόσο στην ατομική ιδιωτικότητα όσο και στην ασφάλεια των συστημάτων πληροφορικής. Μερικά από τα μειονεκτήματα είναι:

1. **Ιδιωτικότητα και Εμπιστευτικότητα Δεδομένων**: Η εγκατάσταση κατασκοπευτικού λογισμικού μπορεί να παραβιάσει την ιδιωτικότητα των χρηστών, καθώς συλλέγει πληροφορίες χωρίς τη συγκατάθεσή τους. Αυτό μπορεί να προκαλέσει σοβαρές παραβιάσεις της ιδιωτικής ζωής.
2. **Παραβίαση της ιδιωτικής ζωής**: Η εγκατάσταση κατασκοπευτικού λογισμικού σε συσκευές χωρίς τη συγκατάθεση των χρηστών παραβιάζει την ιδιωτική τους ζωή, καθώς παρακολουθεί και καταγράφει τις επικοινωνίες και άλλα δεδομένα χωρίς τη γνώση τους.
3. **Κίνδυνος για την ατομική ασφάλεια**: Η χρήση κατασκοπευτικού λογισμικού μπορεί να απειλήσει την ατομική ασφάλεια των ατόμων, καθώς μπορεί να εκτίθενται σε επικίνδυνες καταστάσεις εάν τα προσωπικά τους δεδομένα πέσουν σε λάθος χέρια ή εκμεταλλευτούν από κακόβουλους.
4. **Απειλή για τη δημοκρατία και τα ανθρώπινα δικαιώματα**: Η χρήση κατασκοπευτικού λογισμικού από κυβερνήσεις και αρχές επιβολής νόμου για παρακολουθήσεις δημοσιογράφων, ακτιβιστών και πολιτικών αντιπάλων μπορεί να απειλήσει τη δημοκρατία και τα ανθρώπινα δικαιώματα, καθώς υπονομεύει την

ελευθερία της έκφρασης και την ικανότητα των ατόμων να εκφράζουν ελεύθερα τις απόψεις τους.

5. **Ασφάλεια Συστημάτων**: Το κατασκοπευτικό λογισμικό μπορεί να χρησιμοποιηθεί για να εισβάλλει σε υπολογιστικά συστήματα και να προκαλέσει κακόβουλη δραστηριότητα. Αυτό μπορεί να οδηγήσει σε διαρροές δεδομένων, κλοπή ταυτότητας χρηστών, κλοπή προσωπικών δεδομένων (αριθμοί πιστωτικών/χρεωστικών καρτών , κωδικούς πρόσβασης κλπ) και άλλες απειλές για την κυβερνοασφάλεια.
6. **Εργασιακό Περιβάλλον**: Σε εργασιακά περιβάλλοντα, η χρήση κατασκοπευτικού λογισμικού μπορεί να δημιουργήσει αίσθημα ανασφάλειας μεταξύ των εργαζομένων. Η παρακολούθηση των δραστηριοτήτων τους , **χωρίς την συναίνεση τους** , μπορεί να επηρεάσει αρνητικά την εργασιακή απόδοσή τους και το εργασιακό κλίμα να μην είναι το κατάλληλο για την εξέλιξη των εργαζομένων.
7. **Ανθρώπινες Σχέσεις**: Η χρήση κατασκοπευτικού λογισμικού σε προσωπικές σχέσεις μπορεί να οδηγήσει σε καταστάσεις όπου παραβιάζεται η εμπιστοσύνη. Αυτό μπορεί να καταστρέψει σχέσεις και να προκαλέσει ψυχολογική φθορά.
8. **Νομικές Συνέπειες**: Η χρήση κατασκοπευτικού λογισμικού μπορεί να έχει σοβαρές νομικές συνέπειες, συμπεριλαμβανομένων παραβιάσεων πνευματικών δικαιωμάτων, παραβιάσεων ατομικών δικαιωμάτων και ποινικών κατηγοριών.

Ωστόσο, μία ακόμα βασική ανησυχία του κατασκοπευτικού λογισμικού, εκτός από την παραβίαση της ιδιωτικότητας, είναι η κατανάλωση υπολογιστικών πόρων καθώς εκτελείται στο παρασκήνιο των υπολογιστών. Συχνά εκτελείται κρυφά, έτσι ώστε ο χρήστης (θύμα) να μην μπορεί να ανιχνεύσει ότι εκτελείται και η πρώτη ένδειξη του χρήστη ότι το spyware μπορεί να εκτελείται σε ένα σύστημα είναι ότι η απόδοση του συστήματος του μειώνεται σημαντικά για μη εμφανή λόγο. Οι εργασίες που έπαιρναν μερικά δευτερόλεπτα τώρα μπορεί να διαρκέσουν πολύ περισσότερο καθώς ο υπολογιστής περιμένει να ελευθερωθούν οι πόροι που καταναλώνονται από το λογισμικό υποκλοπής spyware. Όταν ένας χρήστης έχει πολλές περιπτώσεις κακόβουλου λογισμικού που εκτελούνται ταυτόχρονα, τότε το πρόβλημα θα μεγεθύνεται ακόμη περισσότερο. Οι χρήστες μπορούν στη συνέχεια να ανασυγκροτήσουν τους σκληρούς δίσκους τους ή να πραγματοποιήσουν άλλη συντήρηση χωρίς αποτέλεσμα. Επιπλέον, όσο δύσκολο και αν είναι ο εντοπισμός του λογισμικού αυτού, μπορεί να είναι ακόμη πιο δύσκολο να αφαιρεθεί.

Συνολικά, η χρήση κατασκοπευτικού λογισμικού έχει ευρείες και σοβαρές επιπτώσεις σε πολλούς τομείς της κοινωνίας και της τεχνολογίας. Είναι σημαντικό να λαμβάνονται υπόψη οι συνέπειες αυτές κατά την ανάπτυξη, τη χρήση και την ρύθμιση του κατασκοπευτικού λογισμικού.

Κεφάλαιο 7: Προληπτικά Μέτρα Κατά του Κατασκοπευτικού Λογισμικού: Προστατευόμενοι από Ψηφιακές Απειλές.

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο, οι επιπτώσεις της ύπαρξης κατασκοπευτικού λογισμικού είναι αρκετά μεγάλες τόσο για το άτομο όσο και για το σύνολο της κοινωνίας. Η πρόληψη είναι πάντα καλύτερη της θεραπείας, οπότε θα αναφερθούμε αρχικά σε τεχνικές αποφυγής και πρόληψης:

1. **Εγκατάσταση λογισμικού αντι-κατασκοπείας (Anti-spyware)**: Η ασφάλεια ενός λειτουργικού συστήματος δεν είναι πάντοτε αρκετή για την αντιμετώπιση του κακόβουλου αυτού λογισμικού. Οπότε χρειάζεται η εγκατάσταση λογισμικού που ειδικεύεται στην πρόληψη και εξάλειψή αυτού.

2. **Συχνή αναβάθμιση και ενημέρωση του λειτουργικού συστήματος και του λογισμικού αντι-κατασκοπείας (Anti-spyware)**: Το κατασκοπευτικό λογισμικό αναβαθμίζεται δυναμικά μέρα την μέρα βάση των νέων αδυναμιών που βρίσκουν οι επιτιθέμενοι στα λειτουργικά συστήματα. Από την άλλη μεριά οι εταιρείες βρίσκουν σε ποιες αδυναμίες χτυπάνε τα νέα αυτά λογισμικά οπότε βγάζουν νέες ενημερώσεις που οφείλουμε να τις εγκαθιστούμε με σκοπό να αποτρέψουμε τα νέα είδη κακόβουλου λογισμικού. Το ίδιο ισχύει και για τα λογισμικά που έχουμε για την προστασία εναντίον του κατασκοπευτικού λογισμικού.

3. **Αποφυγή χρήσης συνδέσμων**: Πολλές επιθέσεις γίνονται δια μέσω συνδέσμων που στέλνονται στο ηλεκτρονικό ταχυδρομείο ή σε μορφή μηνύματος και με το απλό πάτημά τους εγκαθίσταται κατασκοπευτικό λογισμικό στη συσκευή μας. Άρα οφείλει ο μέσος χρήστης να αποφεύγει το κατά δυνατόν τη χρήση αυτών των συνδέσμων.

4. **Εγκατάσταση μόνο εγκεκριμένων εφαρμογών**: Όπως έχουμε δει βασικό είδος κατασκοπευτικού λογισμικού είναι ο "Δούρειος Ίππος", οπότε θα πρέπει να κατεβάζουμε μόνο από έγκυρους εκδότες και ιστοσελίδες εφαρμογές ώστε να αποφύγουμε την πιθανή εγκατάσταση του εν λόγω κακόβουλου λογισμικού.

5. **Χρήση φιλτραρίσματος περιεχομένου ιστοσελίδων**: Με τη χρήση φιλτραρίσματος περιεχομένου αποφεύγουμε την επίσκεψη σε ιστοσελίδες που θεωρούνται επικίνδυνες. Χρήσιμο επιπλέον θα ήταν να γίνεται ο έλεγχος της ηλεκτρονικής διεύθυνσης της ιστοσελίδας ώστε σε περίπτωση που βρίσκεται σε μια λίστα μη εμπιστών ιστοσελίδων να εμφανίζεται η ανάλογη ειδοποίηση και να μην επιτρέπεται η επίσκεψη αυτής.

6. **Χρησιμοποίηση εφαρμογής μπλοκαρίσματος αναδυόμενων διαφημίσεων**: Είναι μια πολύ χρήσιμη εφαρμογή που αποτρέπει το λογισμικό διαφημίσεων να δράσει, καθώς αποτρέπεται η εμφάνιση αναδυόμενων διαφημίσεων στον διαδικτυακό χώρο. Αυτό κάνει πιο ευχάριστη την πλοήγηση και επίσης λόγω του ότι πολλές από αυτές τις

διαφημίσεις κάνουν ανακατεύθυνση σε άλλες διαδικτυακές διευθύνσεις, προστατεύει τον χρήστη από την επίσκεψη των πιθανά κακόβουλων διαδικτυακών τοποθεσιών.

7. **Προσεκτική απονομή δικαιωμάτων**: Οι περισσότερες εφαρμογές ζητούν συνήθως άδειες για την ομαλή λειτουργία τους. Παρόλα αυτές πολλές φορές ζητάνε παραπάνω άδειες από τις απαραίτητες, γεγονός που ο χρήστης οφείλει να αποτρέπει (κάμερα, μικρόφωνο κ.λπ.) για να αποφύγει την πιθανή παρακολούθησή του.

Αυτά τα μέτρα πρόληψης θα μπορέσουν σε ένα μεγάλο βαθμό να προστατέψουν κάθε χρήστη σε περίπτωση που τα εφαρμόσει. Αλλά είναι αντιληπτό ότι δεν είναι εφικτή πάντα η πρόληψη και φτάνουμε στο σημείο που η συσκευή μας θα έχει μολυνθεί από κατασκοπευτικό λογισμικό. Τα σημάδια αυτής της μόλυνσης στο μεγαλύτερο ποσοστό των περιπτώσεων βρίσκονται στην παρακάτω λίστα:

1. **Μικρότερη απόδοση συστήματος**: Συγκεκριμένα κατασκοπευτικά λογισμικά χρησιμοποιούν αρκετούς πόρους του συστήματος κάνοντας το πιο αργό.

2. **Εμφάνιση πολλών αναδυόμενων διαφημίσεων**: Εμφανίζονται πολλές διαφημίσεις στην αρχική οθόνη ή λογισμικά περιήγησης.

3. **Δυσκολία σύνδεσης σε έγκυρες ιστοσελίδες**: Το λογισμικό χρησιμοποιεί φαινομενικά έγκυρες ιστοσελίδες με σκοπό να υποκλέψει τα στοιχεία σύνδεσης του χρήστη.

4. **Μη λειτουργία λογισμικού ασφαλείας**: Το καλά σχεδιασμένο κακόβουλο λογισμικό έχει ως πρωταρχική λειτουργία την απενεργοποίηση των μηχανισμών ασφαλείας ώστε να μην μπορεί να εντοπίσει.

5. **Εμφάνιση νέων μη πιστοποιημένων εφαρμογών**: Μπορεί κατά την ενδεχόμενη έρευνα να βρεθούν εφαρμογές που δεν έχουν εγκατασταθεί από τον χρήστη.

6. **Εμφάνιση νέων γραμμών εργαλείων**: Κατά την επίσκεψη μας σε μια εφαρμογή περιήγησης παρατηρεί ο χρήστης νέα εργαλεία που δεν έχει εγκαταστήσει ο ίδιος.

7. **Αποστολή αρχείων προς τρίτη πηγή**: Ο χρήστης παρατηρεί ότι πολλά αρχεία ή ένα κρυπτογραφημένο φεύγουν από τον υπολογιστή με παραλήπτη έναν τρίτο που μπορεί να είναι προσωπικές πληροφορίες ή αρχείο με τα δεδομένα εισόδου πληκτρολογίου (key-logging file).

Έχοντας παρατηρήσει τα παραπάνω σημάδια στη συσκευή, οφείλουμε να πάμε στο επόμενο στάδιο, που είναι η εύρεση του κατασκοπευτικού λογισμικού που βρίσκεται εντός της συσκευής. Υπάρχουν διάφοροι τρόποι εύρεσης αυτού, που ορισμένοι μπορεί να χρησιμοποιούνται και από λογισμικά αντι-κατασκοπείας για πρόληψη. Οι τεχνικές αυτές είναι οι τέσσερις παρακάτω:

1. **<u>Ανίχνευση βάσει υπογραφής λογισμικού</u>**: Σε αυτή τη μέθοδο βρίσκουμε την ύπαρξη κατασκοπευτικού λογισμικού συγκρίνοντας την υπογραφή του λογισμικού με τις υπογραφές ήδη γνωστών κατασκοπευτικών λογισμικών. Οι συγκεκριμένες υπογραφές δημιουργούνται μέσω της ανάλυσης του κώδικα του λογισμικού σε δυαδικό σύστημα, βρίσκοντας αν ανήκει σε κάποια οικογένεια κακόβουλων λογισμικών. Βασικό πλεονέκτημα αυτής είναι η υψηλή ακρίβεια στην εύρεση αυτών. Από την άλλη όμως μειονέκτημα αποτελεί ότι ένα νέο κατασκοπευτικό λογισμικό δεν θα είναι καταχωρημένο, οπότε δεν θα αντιστοιχεί πουθενά η υπογραφή του.

2. **<u>Ανίχνευση βάση συμπεριφοράς λογισμικού</u>**: Σε αυτή την τεχνική πρακτική αναλύουμε τη συμπεριφορά των λογισμικών. Το αρχικό στάδιο είναι η εύρεση μιας συμπεριφοράς του συστήματος όπου βρίσκεται σε ασφαλή κατάσταση και την ορίζουμε ως την κανονική κατάσταση του συστήματος. Έπειτα σε δεύτερο στάδιο γίνεται η σύγκριση μεταξύ της κανονικής κατάστασης και της κατάστασης μετά την επίθεση. Η διαφορά μεταξύ αυτών των δύο συμπεριφορών ορίζεται ως πιθανή απειλή. Βασικό πλεονέκτημα αποτελεί ότι μπορεί να ανιχνευθούν και καταγεγραμμένα και μη καταγεγραμμένα κατασκοπευτικά λογισμικά. Αλλά από την άλλη, μειονέκτημα αποτελεί η ανάγκη συνεχούς ενημέρωσης των δεδομένων που ορίζουν την κανονική συμπεριφορά ενός συστήματος. Η ενημέρωση αυτή απαιτεί αρκετούς πόρους για τη διεκπεραίωσή της. Επίσης, αποτελεί ζήτημα προβληματισμού το ότι υπάρχουν υψηλά ποσοστά ψευδών αληθών καταστάσεων.

3. **<u>Ανίχνευση βάση προδιαγραφής λογισμικού</u>**: Αυτή η τεχνική πρακτική προσπαθεί να βελτιώσει το πρόβλημα της ψευδούς αληθούς κατάστασης της προηγούμενης τεχνικής. Σε αυτήν έχουμε ως γνώμονα το ποσοστό διαφοράς της συμπεριφοράς από την αρχική κατάσταση, και όχι την αντιστοίχιση και εύρεση της εκτέλεσης μιας συγκεκριμένης επίθεσης. Βασικό πλεονέκτημα αποτελεί ότι μπορεί να βρει καταγεγραμμένους και μη κινδύνους. Από την άλλη, βασικό μειονέκτημα είναι η υψηλή ύπαρξη της ψευδούς αρνητικής κατάστασης, οπότε σε σχέση με την προηγούμενη είναι πιο δύσκολο να βρει νέες μη καταγραμμένες επιθέσεις. Επιπροσθέτως, πρέπει να σημειωθεί ότι ανάλογα με την ακρίβεια του μοντέλου, απαιτείται και η ανάλογη δέσμευση των πόρων.

4. **<u>Ανίχνευση βάση εξόρυξης δεδομένων</u>**: Σε αυτήν την αρχικά συλλέγουμε δεδομένα και μέσω στατιστικής ανάλυσης βρίσκουμε συγκεκριμένα μοτίβα και ενδείξεις. Έπειτα, με τη χρήση της μηχανικής μάθησης και βάση της προηγούμενης μπορούμε να βρούμε έναν ταξινομητή που χωρίζει σε κλάσεις τις πιθανές περιπτώσεις. Έτσι, θα έχουμε δημιουργήσει ένα μοντέλο που είναι ικανό στην ανίχνευση και εύρεση νέων ή και μη υπαρκτών κατασκοπευτικών λογισμικών. Αυτή η τεχνική έχει το μεγαλύτερο ποσοστό ανίχνευσης σε σχέση με τις προηγούμενες τρεις.

Βάσει της εκτέλεσης ενός ή περισσότερων από αυτές τις τεχνικές, θα έχουμε τη δυνατότητα, πιθανώς, να εντοπίσουμε το κατασκοπευτικό λογισμικό που έχει εγκατασταθεί/υπάρχει στον υπολογιστή μας. Έχοντας ως στόχο να το καταπολεμήσουμε, η "θεραπεία" του υπολογιστή από αυτού του είδους το κακόβουλο λογισμικό μπορεί να γίνει

με διάφορους τρόπους ανάλογα με το είδος του κατασκοπευτικού λογισμικού. Μερικοί από αυτούς τους τρόπους περιλαμβάνουν:

1. **Χρήση αμυντικής ασφάλειας λειτουργικού συστήματος:** Τα περισσότερα λειτουργικά συστήματα της εποχής έχουν ένα δικό τους σύστημα ασφάλειας αλλά και ένα δικό τους λογισμικό για την καταπολέμηση του κακόβουλου λογισμικού. Με την ενεργοποίηση αυτού, μπορούμε να εντοπίσουμε τον κατασκοπευτικό λογισμικό που έχει μολύνει τη συσκευή μας, αλλά οι δυνατότητες αυτών είναι περιορισμένες καθώς βασίζονται κιόλας στο ήδη υπάρχον αναχώματα ασφάλειας που υποτίθεται αποτρέπει την είσοδο αυτών.

2. **Χρήση λογισμικού αφαίρεσης κατασκοπευτικού λογισμικού:** Τα γνωστά και ως αντικατασκοπευτικά λογισμικά (Anti-spyware software) αποτελούν ένα πιο δυνατό μέσο από την πρώτη επιλογή για την εξάλειψη του κακόβουλου λογισμικού. Τις περισσότερες φορές είναι πιο αποδοτικό και εξειδικευμένο από το λειτουργικό σύστημα, αλλά αυτό βασίζεται στο κόστος αυτού.

3. **Χειροκίνητη αφαίρεση κατασκοπευτικού λογισμικού:** Είναι η πιο αναξιόπιστη λύση σε σχέση με τις προηγούμενες. Πρακτικά, σε αυτήν επανεκκινείς τη συσκευή σε "ασφαλή λειτουργία" και σε αυτή θα διαγράψεις τα ύποπτα αρχεία και έπειτα θα ελέγξεις ποιες εφαρμογές έχουν εγκατασταθεί πρόσφατα και θα τις διαγράψεις καθώς είναι το πιο πιθανό το κατασκοπευτικό λογισμικό να έχει εγκατασταθεί πρόσφατα. Τέλος, επιστρέφουμε στην κανονική λειτουργία του υπολογιστή.

Αυτές είναι οι πιο κοινές λύσεις για τη διαγραφή/αντιμετώπιση του κατασκοπευτικού λογισμικού στη συσκευή μας. Πιο αποτελεσματική, θα μπορούσαμε να πούμε ότι αποτελεί η δεύτερη καθώς με την καλή αγορά ενός τέτοιου προγράμματος, λόγω της εξειδίκευσης αυτού, είναι πιο πιθανό να αναγνωρισθεί το κατασκοπευτικό λογισμικό και στη συνέχεια να αφαιρεθεί.

Κεφάλαιο 8: Περιπτώσεις χρήσης Κατασκοπευτικού Λογισμικού (Case Studies)

Μέσα από τις ακόλουθες περιπτώσεις, καταλαβαίνουμε πώς το κατασκοπευτικό λογισμικό χρησιμοποιείται σε πρακτικές , επιχειρησιακές και γεωπολιτικές συνθήκες.

Κάθε περίπτωση αναλύεται λεπτομερώς, προσφέροντας μια εικόνα των συνεπειών και των επιπτώσεων που προκύπτουν από τη χρήση του κατασκοπευτικού λογισμικού. Από την NSO Group στην Ισραήλ, μέχρι τη DarkMatter στα Ηνωμένα Αραβικά Εμιράτα, καθώς και τον ρωσικό ανάδοχο του Υπουργείου Άμυνας ENFER, ανακαλύπτουμε πώς αυτές οι οντότητες χρησιμοποιούν το κατασκοπευτικό λογισμικό για τους δικούς τους σκοπούς.

Περίληψη υποθέσεων που θα αναλύσουμε

Μελέτη Περίπτωσης	**Χώρα προέλευσης**	**Έτος Ίδρυσης**	**Βασικοί Πελάτες**
NSO GROUP	Ισραήλ	2016	Παγκόσμιοι
ENFER	Ρωσία	Άγνωστο	Ρωσία
DarkMatter	Αραβικά Εμιράτα	2016	Αραβικά Εμιράτα

1. NSO GROUP

Η NSO Group, πιθανώς η πιο διάσημη από τις τρεις περιπτώσεις μελέτης, είναι μια ισραηλινή εταιρεία που κατηγορείται ότι εκμεταλλεύεται εταιρείες τεχνολογίας των Ηνωμένων Πολιτειών για να κατασκοπεύει τα άτομα που διαφωνούν με τη δράση της κυβέρνησης , όπως για παράδειγμα δημοσιογράφους, ακτιβιστές, πολιτικούς αντιπάλους, και άλλες ομάδες ή άτομα που θεωρούνται απειλή για το καθεστώς ή τα συμφέροντα της συγκεκριμένης κυβέρνησης. Η NSO Group είναι μια ισραηλινή εταιρεία που ιδρύθηκε το 2010 από πρώην μέλη των ισραηλινών μυστικών υπηρεσιών. Η εταιρεία πουλάει το προϊόν κατασκοπείας Pegasus, σε πολλαπλές υπηρεσίες πληροφοριών στη Μέση Ανατολή, την Ευρώπη και τη Νότια Αμερική. Το Pegasus επιτρέπει την πρόσβαση τρίτων σε συγκεκριμένες κινητές συσκευές, χωρίς τη γνώση ή την άδεια του χρήστη της συσκευής αυτής, και λειτουργεί για να αποφεύγει τα αντίμετρα που στοχεύουν στην πρόληψη τέτοιας πρόσβασης, με τελικό σκοπό να εξάγει μια ευρεία γκάμα πληροφοριών που υπάρχουν σε αυτήν τη συσκευή. Αυτό σημαίνει ότι η NSO Group, ως εταιρεία κατασκόπευσης, παρέχει την τεχνολογία και τις υπηρεσίες της σε κυβερνήσεις που τις χρησιμοποιούν για να

παρακολουθήσουν ατομικούς ή ομαδικούς αντιφρονούντες εντός των συνόρων τους ή ακόμα και εκτός τους, ανάλογα με το πού εντοπίζονται οι στόχοι.

Μια αγωγή που κατέθεσε η Διεθνής Αμνηστία με στόχο την ανάκληση της άδειας εξαγωγής της NSO Groups απορρίφθηκε από ένα ισραηλινό δικαστήριο τον Ιούλιο του 2020, με τον δικαστή να αναφέρεται στις διαδικασίες ελέγχου βάσει των ανθρωπίνων δικαιωμάτων τόσο πριν όσο και μετά την πώληση. Η NSO Group επιτρέπεται λοιπόν να λειτουργεί από τη χώρα στην οποία εδρεύει - πράγματι, έχει στενούς δεσμούς με τις ισραηλινές στρατιωτικές και πληροφοριακές υπηρεσίες, όπως πολλές άλλες κυβερνοαμυντικές και επιθετικές εταιρείες στον κυβερνοχώρο του Ισραήλ.

Οι δραστηριότητες της NSO Group είναι δημόσιες κυρίως λόγω της ερευνητικής εργασίας του Citizen Lab, μιας καναδικής ερευνητικής οργάνωσης με έδρα το Πανεπιστήμιο του Τορόντο. Σε μία έκθεση του το 2018, το Citizen Lab εντόπισε διακομιστές που επικοινωνούσαν με το κακόβουλο λογισμικό Pegasus της NSO που ανήκαν σε τριάντα έξι διαφορετικούς φορείς σε όλο τον κόσμο - πιθανώς ξεχωριστές υπηρεσίες ασφαλείας ή πληροφοριών. Πολλοί από αυτούς τους φορείς βρίσκονται σε κράτη με άσχημα ανθρώπινα δικαιώματα και υπάρχουν προηγούμενες ενδείξεις εξειδικευμένης παρακολούθησης εναντίον πολιτικής αντιπολίτευσης, δημοσιογράφων και διαφωνούντων.

Οι δηλώσεις της εταιρείας υποδεικνύουν συνεχώς ότι η NSO Group δεν λαμβάνει αποφάσεις σχετικά με το ποιους να στοχεύσει, και αυτό υποστηρίζεται από δημόσιες πληροφορίες σχετικά με τους στόχους. Πράγματι, ο όρος (Access-as-a-Service) Πρόσβαση-ως-Υπηρεσία υπονοεί ότι αυτή είναι ίσως η μοναδική απόφαση που απαιτείται από τον χρήστη της υπηρεσίας. Όσον αφορά τον έλεγχο και τον συντονισμό κατά τη διάρκεια μιας παρακολούθησης, η εταιρεία επιμένει ότι δεν διεξάγει καθόλου βοήθεια στον πελάτη. Είναι δύσκολο να γνωρίζουμε με βεβαιότητα αν αυτό συμβαίνει στην πραγματικότητα για διάφορους λόγους. Διαρροές εγγράφων υποδεικνύουν ότι συνεργάζονται στενά με άλλες εταιρείες που παρέχουν συμπληρωματικές ικανότητες σε πελάτες, και δεν είναι σαφές ποια επιρροή έχουν σε αυτήν τη διαδικασία.

Η NSO Group παρέχει εκτεταμένη εκπαίδευση και υποστήριξη στους πελάτες της. Αυτή περιλαμβάνει αρχικές επιδείξεις της τεχνολογίας της, αναφορικά με τις συσκευές των στόχων που επιλέγονται από τον πελάτη, μέχρι εκπαίδευση στη χρήση της τεχνολογίας αυτής από τους χειριστές του πελάτη. Επίσης προσφέρει συνεχή υποστήριξη επί τόπου από μηχανικούς, επίλυση προβλημάτων και αντιμετώπιση τεχνικών προβλημάτων με το λογισμικό εάν προκύψουν.

2. ENFER

ENFER είναι το ψευδώνυμο που υπάρχει για μια ρωσική εταιρεία παροχής κυβερνοασφάλειας που βοηθά τις ρωσικές υπηρεσίες πληροφοριών στις επιθετικές της κυβερνοεπιχειρήσεις, αναπτύσσοντας δυνατότητες που η Ρωσία μπορεί να αποφασίσει να χρησιμοποιήσει εναντίον στρατηγικών αντιπάλων. Είναι ενεργή στη ρωσική αγορά και σε αρκετά γραφεία παγκοσμίως, τα οποία δημοσίως προσφέρουν υπηρεσίες ελέγχου κώδικα, δοκιμών διείσδυσης και προσομοίωσης απειλών, ανακάλυψης και διαχείρισης ευπαθειών, ανίχνευσης και αντιμετώπισης απειλών, καθώς και υπηρεσίες πληροφοριών για επιχειρήσεις και κυβέρνηση, μαζί με σχετικές υπηρεσίες εκπαίδευσης. Η εταιρεία έχει αναγνωρίσει το Υπουργείο Άμυνας της Ρωσικής Ομοσπονδίας ως έναν από τους πρώτους

πελάτες της, έχοντας επίσημα δημιουργήσει μια σχέση μέσα στα πρώτα δύο χρόνια από την ίδρυση της εταιρείας. Αυτή η σχέση ενισχύθηκε περαιτέρω από αδιευκρίνιστη συνεργασία με τις υπηρεσίες ασφαλείας τα τελευταία δέκα χρόνια.

Οι εργαζόμενοι της ENFER και άλλοι ρωσικοί ειδικοί κυβερνοασφάλειας έχουν περιγράψει τις δραστηριότητες της εταιρείας ως παροχή πλατφόρμας για ανάπτυξη δυνατοτήτων και πρόσβαση. Αναφέρεται ότι η εταιρεία αναπτύσσει και υποστηρίζει επιθετικές δυνατότητες και λειτουργίες για πολλούς πελάτες, περιλαμβάνοντας εργασίες αντίδρασης σε άμεσα αιτήματα αξιωματούχων του FSB (υπηρεσία ασφαλείας της Ρωσίας) σε συγκεκριμένα έργα που αφορούν επιθετικές δραστηριότητες, συμπεριλαμβανομένης της ανακάλυψης και ενοποίησης εκμετάλλευσης ευπαθειών, ανάπτυξης κακόβουλου λογισμικού και μηχανικής υποδομής.

Όπως και η NSO Group, η ENFER, επιτρέπεται να λειτουργεί στη χώρα στην οποία βρίσκεται.

Η ENFER διεξάγει μοναδική έρευνα εντοπισμού ευπαθειών και περαιτέρω μηχανική για την ανάπτυξη αξιόπιστου κώδικα εκμετάλλευσης που στοχεύει σε αυτές τις ευπάθειες. Αυτές οι ευπάθειες 0day (zero day) περιγράφονται ως προοριζόμενες για χρήση σε δραστηριότητες δοκιμής διείσδυσης και άλλες επιθέσεις ασφαλείας. Ωστόσο, αυτές οι ικανότητες παρέχονται επίσης σε πελάτες της ρωσικής κυβέρνησης.

Η ENFER αναφέρεται ότι έχει αναπτύξει πολλαπλές παραλλαγές κακόβουλου λογισμικού για επιθετική χρήση, συμπεριλαμβανομένης της εισβολής σε συστήματα και της κλοπής εγγράφων, για λογαριασμό της FSB. Αυτή η σχέση είναι συνδεδεμένη με άλλες αλληλεπιδράσεις μεταξύ της FSB και των συνεργατών της, συμπεριλαμβανομένων της InformInvestGroup και της ODT LLC. Αυτές οι οντότητες ανέπτυξαν την οικογένεια κακόβουλου λογισμικού FRONTON, με σκοπό να διαρρεύσουν ευπαθείς συσκευές Internet of Things (IoT) για να παρέχουν επιθετικές κυβερνοεπιθέσεις απόρριψης υπηρεσιών (DDoS). Το 2^{ο} κέντρο της FSB, Κέντρο Πληροφοριών Ασφάλειας (επίσης γνωστό ως Κέντρο 18 ή με την κωδική ονομασία 64829 μονάδας κάλυψης), αναγνωρίστηκε ως ο τελικός πελάτης για αυτό το λογισμικό.

Σύμφωνα με πληροφορίες, οι υπάλληλοι της ENFER συμμετείχαν άμεσα στη διαχείριση συστημάτων και είχαν τον έλεγχο των αναπτυγμένων δυνατοτήτων πρόσβασης εισβολής. Ειδικότερα, το προσωπικό της ENFER φέρεται να ήταν κρίσιμο για τις ενέργειες στο εξωτερικό, όπου οι αξιωματικοί της FSB δεν λειτουργούσαν απευθείας επί τόπου σε άλλες εταιρείες.

Ο βαθμός στον οποίο το προσωπικό της ENFER έχει εμπλακεί στον προγραμματισμό και τη διαχείριση των λειτουργιών παραμένει ασαφές. Σε πολλές περιπτώσεις, το προσωπικό της ENFER μπορεί να έχει εμπλακεί σε επιχειρήσεις που δεν εκτελούνται υπό την καθοδήγηση ενός κράτους.Τέτοια διαφθορά έχει σημειωθεί προηγουμένως σε μεγάλες υποθέσεις που αφορούν αξιωματικούς της FSB.

Στα τέλη του 2016, πολλοί αξιωματικοί της FSB και ένας εργαζόμενος που εργαζόταν για μια διαφορετική εταιρεία κυβερνοασφάλειας συνελήφθησαν με κατηγορίες που περιελάμβαναν κατηγορίες για εμπλοκή σε δραστηριότητες εγκλήματος στον κυβερνοχώρο.

Η ENFER παρέχει πολλαπλές υπηρεσίες εκπαίδευσης σε Ρώσους και άλλους κυβερνητικούς πελάτες, καθώς και σε εταιρείες του ιδιωτικού τομέα. Πολλές από αυτές τις εκπαιδευτικές δραστηριότητες είναι εστιασμένες αποκλειστικά σε επιθετικούς στόχους.

3. **DARKMATTER GROUP**

Η DarkMatter Group (επίσης γνωστή και ως DarkMatter LLC ή απλώς "DarkMatter") είναι μια εταιρεία κυβερνοασφάλειας με έδρα τα Ηνωμένα Αραβικά Εμιράτα. Αρχικά ιδρύθηκε από ανάδοχους της αμερικανικής κυβέρνησης για να βοηθήσει τα ΗΑΕ να αναπτύξουν κυβερνο-δυνατότητες, ωστόσο πλέον έχει πραγματοποιήσει επιχειρήσεις εναντίον πολιτών των ΗΠΑ και προσλαμβάνει δυτικούς ερευνητές ασφάλειας για να ενισχύσει τις δυνατότητες κατασκοπείας της. Σύμφωνα με ανοικτές πηγές, η DarkMatter είναι επίσης στενά εμπλεκόμενη στις αποφάσεις λήψης στόχων σε επιχειρησιακό επίπεδο.

Η εταιρεία DarkMatter Group προσφέρει τέσσερις ξεχωριστές υπηρεσίες:

- Το ψηφιακό και εφαρμοσμένο τμήμα τεχνολογίας (με την ονομασία DigitalX1) που δηλώνει ότι βοηθάει επιχειρήσεις και κυβερνήσεις στη χρήση προηγμένων τεχνολογιών.
- Ένα εκπαιδευτικό τμήμα (DigitalE1) που παρέχει μια ψηφιακή ομάδα ταλέντων για να ενσωματωθεί στους πελάτες εταιριών
- Υπηρεσίες κυβέρνησης που επικεντρώνονται στη βοήθεια των κυβερνήσεων να ενισχύσουν την άμυνα και την ασφάλειά τους μέσω ειδικών τεχνολογιών
- Την ομώνυμη εταιρία Cyber Security and Secure Communications (DarkMatter) που επικεντρώνεται στην ασφάλεια και την ανθεκτικότητα των επιχειρήσεων.

Η εταιρεία εργάζεται κυρίως για την κυβέρνηση των Ηνωμένων Αραβικών Εμιράτων.

Η ιστορική δομή της διαχείρισης της DarkMatter έχει ενδιαφέρον. Η κυβέρνηση των Ηνωμένων Αραβικών Εμιράτων φέρεται να ανέθεσε στην εταιρεία «Project Raven» μια λίστα με στόχους. Οι αμερικανοί υπάλληλοι της Cyberpoint στη συνέχεια εντόπιζαν ευπάθειες στους στόχους, ανέπτυσσαν ή αγοράζαν λογισμικό διείσδυσης και βοηθούσαν στον παρακολούθηση, ενώ η κυβέρνηση των Ηνωμένων Αραβικών Εμιράτων εκτελούσαν στην πραγματικότητα την επίθεση. Αφού η εταιρεία Project Raven εξελίχθηκε σε DarkMatter, η εταιρεία άλλαξε τη διαχειριστική δομή λειτουργίας έτσι ώστε η κυβέρνηση των Ηνωμένων Αραβικών Εμιράτων να εκτελεί παρακολουθήσεις εναντίον πολιτών των ΗΠΑ χωρίς την ενημέρωση των αμερικανικών υπαλλήλων της DarkMatter. Οι διαδικασίες λειτουργικής διαχείρισης της DarkMatter παρέμειναν παρόμοιες με αυτές που παρατηρήθηκαν στην Project Raven για τουλάχιστον έναν από τους κύριους πελάτες της, την Υπηρεσία Σημάτων των ΗΑΕ.

Η DarkMatter παρέχει δημόσια μαθήματα στη βιομηχανία επαγγελματιών σχετικά με "Επιθετικές δοκιμές διείσδυσης κινητών ". Επιπλέον, η εταιρεία παρέχει εκπαίδευση και υποστήριξη στους πελάτες της μέσω διαφημιζόμενων βασικών υπηρεσιών. Ως DarkMatter προσλαμβάνει επιθετικά διεθνή ταλέντα, συμπεριλαμβανομένων των επιθετικών ταλέντων ασφαλείας από τις υπηρεσίες πληροφοριών των "ΗΠΑ" και του Ισραήλ.

Κεφάλαιο 9: Συμπεράσματα

Σε αυτή την εργασία προσπαθήσαμε να φωτίσουμε το θέμα του κατασκοπευτικού λογισμικού. Τι είναι, ποιες είναι οι συνέπειές του και τι μπορεί να γίνει για να προστατευτεί κανείς από το λογισμικό αυτό. Όπως είδαμε, ο ορισμός του κατασκοπευτικού λογισμικού επιτρέπει πολλά διαφορετικά είδη κατηγοριών, κυμαίνονται από τα web cookies έως τα key loggers και τα browser hijackers. Το κατασκοπευτικό λογισμικό έχει επίσης διάφορους τομείς χρήσης, τόσο ως νόμιμες εφαρμογές παρακολούθησης όσο και ως παράνομα εργαλεία για κλοπή πληροφοριών. Η απάντησή μας στο ερώτημα "τι είναι κατασκοπευτικό λογισμικό;" πρέπει, συνεπώς, να είναι αρκετά ευρεία. Είναι οποιοδήποτε κομμάτι λογισμικού που, με ή χωρίς δήλωση συναίνεσης του χρήστη, παρακολουθεί τις δραστηριότητες του υπολογιστή και επιτρέπει σε αυτές τις πληροφορίες να γνωστοποιηθούν σε τρίτους.

Επίσης είδαμε ότι ο τρόπος διάδοσης μπορεί να ποικίλει σημαντικά. Στην περίπτωση μας, είδαμε ότι το κατασκοπευτικό λογισμικό διανέμεται εκμεταλλευόμενο ευπάθειες ασφαλείας σε εγκατεστημένο λογισμικό (π.χ. windows ,Ios , Android). Ένα συμπέρασμα που μπορεί κανείς να συνάγει από αυτό είναι ότι, ως χρήστες υπολογιστή, πρέπει να είμαστε προσεκτικοί κρατώντας ενημερωμένο το λογισμικό μας με ενημερώσεις, να είμαστε περιοριστικοί με το ποιο λογισμικό πακέτων κατεβάζουμε και να διατηρούμε εγκατεστημένο.

Ένα άλλο συμπέρασμα που βγάζουμε από αυτή την εργασία είναι ότι το κατασκοπευτικό λογισμικό γίνεται ραγδαία ένας παράγοντας που πρέπει να ληφθεί υπόψη όταν λαμβάνεται υπόψη η ασφάλεια στο διαδίκτυο γενικά. Σήμερα είναι πολλοί οι υπολογιστές που συνδέονται στο Διαδίκτυο και είναι μολυσμένοι με διάφορα είδη κατασκοπευτικού λογισμικού, και οι μελέτες υποδεικνύουν ότι ο αριθμός των μολυσμένων υπολογιστών αυξάνεται. Από αυτό συμπεραίνουμε ότι γίνεται ένα σοβαρό πρόβλημα. Από την άλλη πλευρά, οι πληροφορίες σχετικά με το κατασκοπευτικό λογισμικό και τις επιπτώσεις του δεν είναι κάτι που ο μέσος χρήστης γνωρίζει. Εάν προσπαθήσουμε να κάνουμε μια εκτίμηση για το πώς θα φαίνεται η κατάσταση με το κατασκοπευτικό λογισμικό σε πέντε χρόνια από τώρα, προβλέπουμε ότι το κατασκοπευτικό λογισμικό θα είναι ακόμα πιο μεγάλο πρόβλημα από ό, τι είναι σήμερα, αλλά επίσης οι χρήστες θα έχουν περισσότερες γνώσεις σχετικά με την κατάσταση και θα υπάρχουν περισσότερα εργαλεία στην αγορά για την καταπολέμηση του κατασκοπευτικού λογισμικού.

Σε έναν κόσμο όπου η τεχνολογία διαδραματίζει καθοριστικό ρόλο στην καθημερινότητά μας, η προστασία της ιδιωτικότητας και της ασφάλειας των δεδομένων μας είναι επιτακτική ανάγκη. Η αντιμετώπιση του κατασκοπευτικού λογισμικού απαιτεί συλλογική προσπάθεια από την κοινωνία, τις επιχειρήσεις και τους ιδιώτες χρήστες. Με εκπαίδευση, ευαισθητοποίηση και αποτελεσματικές πρακτικές προστασίας, μπορούμε να δημιουργήσουμε έναν ασφαλέστερο και πιο ιδιωτικό ψηφιακό χώρο για όλους.

Βιβλιογραφία

1. Daniel Jonasson , Johan Sigholm , "*What is Spyware?"*
2. Fernando M. Luna, *"THE PERILS OF SPYWARE"*
3. Paul M. Schwartz, *"Privacy Inalienability and the Regulation of Spyware"*
4. Liying Sun , *"Who Can Fix the Spyware Problem?"*
5. Bethany Rubin Henderson , "*Hey, that's personal! When companies sell customer information gathered through the Internet"*
6. Susan P. Crawford, "*First Do No Harm: The Problem of Spyware*"
7. Patricia L. Bellia, *"Spyware and the Limits of Surveillance Law"*
8. James L. Sipes , *"THE DANGERS OF SPYWARE"*
9. WINNONA DESOMBRE, JAMES SHIRES, JD WORK, ROBERT MORGUS, PATRICK HOWELL O'NEILL, LUCA ALLODI and TREY HERR, "Case Studies"
10. Thomas F. Stafford , Andrew Urbaczewski , *"Spyware: The Ghost in the Machine"*
11. Tamara Dinev, Qing Hu, *"Is Spyware an Internet Nuisance or Public Menace?"*
12. Martin Boldt, Bengt Carlsson & Andreas Jacobsson , *"Exploring Spyware Effects"*
13. Nathaniel Good , Rachna Dhamija , Jens Grossklags , David Thaw , Steven Aronowitz , Deirdre Mulligan , Joseph Konstan , "*Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware"*
14. Rahul Chatterjee , Periwinkle Doerfler , Hadas Orgad , Sam Havron, Jackeline Palmer , Diana Freed , Karen Levy , Nicola Dell∗ , Damon McCoy , Thomas Ristenpart , "*The Spyware Used in Intimate Partner Violence"*
15. Alexander Moshchuk, Tanya Bragin, Steven D. Gribble, and Henry M. Levy, "*A Crawler-based Study of Spyware on the Web*"
16. Sergii Lysenko, Kira Bobrovnikova, Peter Popov Viacheslav Kharchenko, Dmytro Medzatyi , *"Spyware Detection Technique Based on Reinforcement Learning"*
17. Chawla A , *"Pegasus Spyware – 'A Privacy Killer'"*
18. SARAH A. CHERRY , *"The Effects of Spyware and Phishing on the Privacy Rights of Internet Users"*
19. Mayank Agrawal , Gagan Varshney, Saumya , Kaushal Pratap Singh , Manish Verma , *"Pegasus: Zero-Click spyware attack – its countermeasures and challenges"*
20. Martin Boldt, Johan Wieslander , *"Investigating Spyware in Peer-to-Peer Tools"*

21. Caitlin Maslen, *"The implications of spyware and surveillance technology for anticorruption activists"*

22. https://www.spiceworks.com/it-security/security-general/articles/what-is-spyware/

23. https://www.imperva.com/learn/application-security/what-is-spyware/

24. https://www.fortinet.com/resources/cyberglossary/spyware

25. https://www.avast.com/c-spyware

26. https://ieeexplore.ieee.org/abstract/document/8668010

27. https://www.trendmicro.com/vinfo/us/security/definition/adware#:~:text=Adware%2C%20or%20"advertising-supported,are%20actually%20considered%20as%20grayware.

28. https://www.kaspersky.com/resource-center/definitions/keylogger

29. https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus#:~:text=Spy%20Trojan%3A%20Spy%20Trojans%20are,use%2C%20and%20tracking%20login%20data.

30. https://www.kaspersky.com/resource-center/threats/spyware

31. https://www.fortinet.com/resources/cyberglossary/rootkit#:~:text=A%20common%20rootkit%20definition%20is,a%20long%20period%20of%20time.

32. https://www.malwarebytes.com/cybersecurity/computer/what-are-tracking-cookies

33. https://www.malwarebytes.com/blog/threats/mobile-spyware

34. https://allaboutcookies.org/what-is-a-web-beacon

35. https://www.kaspersky.com/resource-center/preemptive-safety/spyware-on-android

36. https://www.kaspersky.com/resource-center/threats/adware

37. https://www.kaspersky.com/resource-center/threats/trojans

38. https://www.legalmatch.com/law-library/article/spyware.html

39. https://www.justice.gov/jm/jm-9-7000-electronic-surveillance

40. https://www.spamlaws.com/spyware-laws.html

41. https://www.empoweringparents.com/article/teens-parents-privacy/

42. https://examonline.in/online-proctoring-an-effective-method-of-monitoring-online-exams/

43. https://www.businessnewsdaily.com/6685-employee-monitoring-privacy.html

44. https://ieeexplore.ieee.org/abstract/document/8328265

45. https://www.kaspersky.com/blog/stalkerware-spouseware/26292/