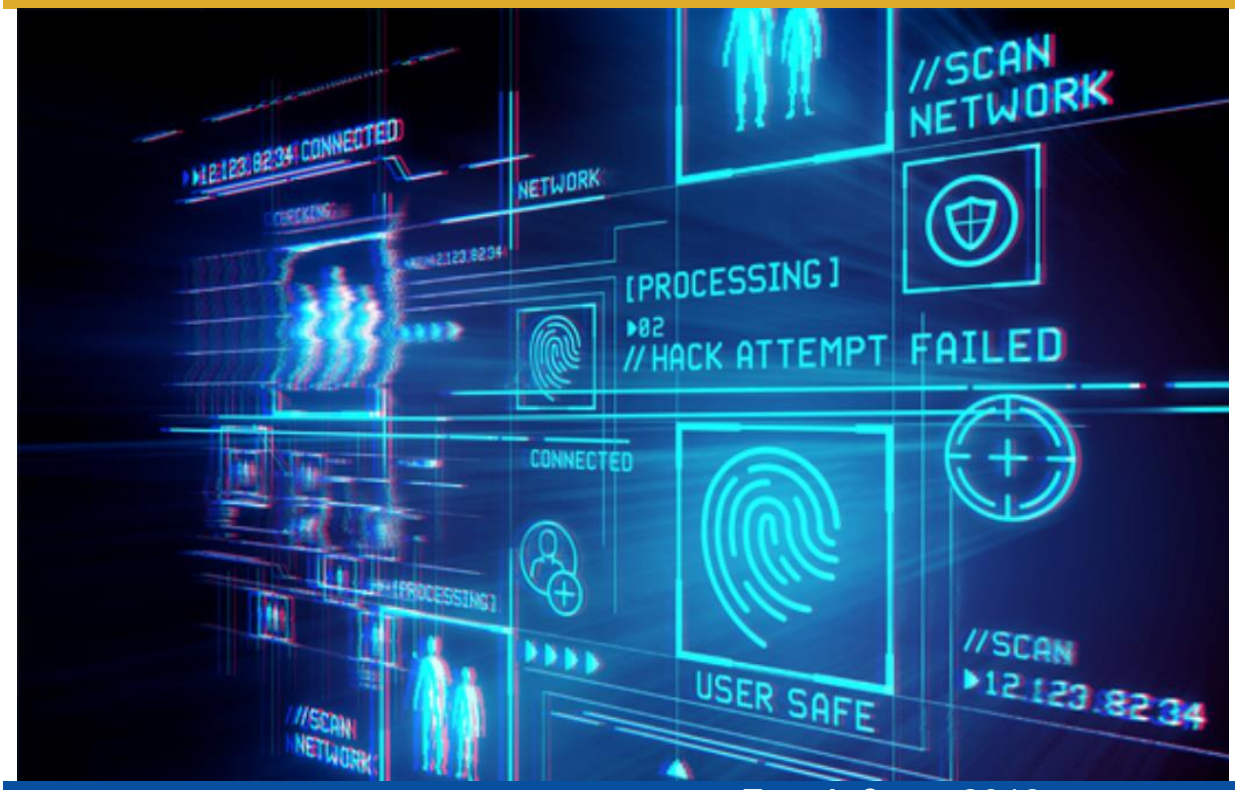
EUIPO
ΓΡΑΦΕΙΟ ΔΙΑΝΟΗΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

ΕΝΤΟΠΙΣΜΟΣ ΚΑΙ ΑΝΑΛΥΣΗ ΤΟΥ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΣΕ ΕΠΙΛΕΓΜΕΝΟΥΣ ΔΙΑΔΙΚΤΥΑΚΟΥΣ ΤΟΠΟΥΣ ΥΠΟΠΤΟΥΣ ΓΙΑ ΠΑΡΑΒΙΑΣΗ ΔΙΚΑΙΩΜΑΤΩΝ ΔΙΑΝΟΗΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

ΠΕΡΙΛΗΨΗ



Σεπτέμβριος 2018

Περίληψη

Το ύποπτο παράνομο περιεχόμενο συνιστά σημαντική παραβίαση των δικαιωμάτων διανοητικής ιδιοκτησίας. Υπάρχουν κάποιοι διαδικτυακοί τόποι που διαθέτουν δημόσια περιεχόμενο του είδους αυτού, ενίοτε ακόμη και δωρεάν, χωρίς εγγραφή. Παράλληλα με αυτό το περιεχόμενο, οι διαδικτυακοί τόποι συνήθως διανέμουν διαφόρων ειδών κακόβουλο λογισμικό και δυνητικά ανεπιθύμητα προγράμματα (potentially unwanted programs, PUP), δελεάζοντας τους χρήστες να μεταφορτώσουν και να τρέξουν τα εν λόγω αρχεία. Στη μελέτη γίνεται μια επισκόπηση των πιο πρόσφατων δειγμάτων κακόβουλου λογισμικού και PUP που βρέθηκαν σε διαδικτυακούς τόπους ύποπτους για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας. Τα προγράμματα αυτά χρησιμοποιούν παραπλανητικές τεχνικές και κοινωνική μηχανική —όπως κενές εφαρμογές εγκατάστασης παιχνιδιών ή φαινομενικά «χρήσιμο» λογισμικό— για να αποσπάσουν δολίως από τους τελικούς χρήστες ευαίσθητα δεδομένα τους. Στη διάρκεια της μελέτης ανακαλύφθηκαν πολλά διαφορετικά PUP, π.χ. δήθεν «χρήσιμο» λογισμικό, απομιμήσεις εφαρμογές εγκατάστασης παιχνιδιών και πελάτες για πλατφόρμες βίντεο συνεχούς ροής. Το λογισμικό αυτό δεν απειλεί κατ' ανάγκη το λογισμικό ή το υλισμικό του χρήστη. Ωστόσο, μέσα από τεχνάσματα κοινωνικής μηχανικής, ο χρήστης μπορεί να πειστεί να αποκαλύψει ευαίσθητα προσωπικά δεδομένα ή στοιχεία καρτών πληρωμών. Εξάλλου, μπορεί να διαρρεύσουν πληροφορίες για τον ίδιο τον υπολογιστή προς τρίτους χωρίς τη ρητή συγκατάθεση του χρήστη.

Ερευνητική ομάδα

Στην ερευνητική ομάδα συμμετείχαν η Francesca Bosco, υπεύθυνη προγραμμάτων του Διαπεριφερειακού ιδρύματος ερευνών των Ηνωμένων Εθνών για το έγκλημα και τη δικαιοσύνη (UNICRI) και ο Andrii Shalaginov, διδακτορικός ερευνητής σε θέματα ασφάλειας των πληροφοριών στο Τμήμα ασφάλειας των πληροφοριών και τεχνολογίας της επικοινωνίας (Ομάδα ψηφιακής εγκληματολογίας), Σχολή πληροφορικής και ηλεκτρολόγων μηχανικών του Επιστημονικού και Τεχνολογικού Πανεπιστημίου της Νορβηγίας.

Δήλωση αποποίησης ευθύνης

Στο πλαίσιο της παρούσας μελέτης, επισημαίνεται ότι αποκλειστικός στόχος της έρευνας ήταν ο καθορισμός των τεχνικών χαρακτηριστικών του κακόβουλου λογισμικού και των PUP τα οποία συναντήσαμε στη διάρκεια της μελέτης και τα οποία θα μπορούσαν να συναντήσουν οι χρήστες του διαδικτύου που αναζητούν περιεχόμενο ύποπτο για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας. Τα δείγματα κακόβουλου λογισμικού και PUP που τεκμηριώθηκαν δεν είναι παρά μόνο ενδεικτικά και στόχος της μελέτης (και των αποτελεσμάτων της) δεν ήταν να εκτιμηθούν συνολικά οι πιθανότητες ή ο κίνδυνος τον οποίο διατρέχει ο χρήστης του διαδικτύου που αναζητά περιεχόμενο ύποπτο για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας να προσβληθεί από κακόβουλο λογισμικό ή PUP.

Πρόλογος

Οι ύποπτες επιγραμμικές δραστηριότητες για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας μπορεί να χρηματοδοτούνται με διάφορα μέσα, όπως συνδρομές, δωρεές, πληρωμές για βοηθητικές υπηρεσίες και έσοδα από επιγραμμική προβολή διαφημίσεων.

Ωστόσο, δεν είναι όλα τα μέσα χρηματοδότησης τόσο ακίνδυνα όσο αυτά που προαναφέρθηκαν. Επί σειρά ετών, η διασπορά της προσβολής από κακόβουλο λογισμικό και από άλλο είδος δυνητικά ανεπιθύμητων προγραμμάτων (PUP) διαδραματίζει σημαντικό ρόλο στη χρηματοδότηση ύποπτων παράνομων δραστηριοτήτων στο διαδίκτυο.

Ο μέσος χρήστης του διαδικτύου αρχίζει να συνειδητοποιεί τους κινδύνους προσβολής όταν επισκέπτεται ύποπτους παράνομους διαδικτυακούς τόπους ή προσπελαύνει εφαρμογές για κινητές συσκευές.

Σύμφωνα με τον πίνακα αποτελεσμάτων του EUIPO για τη νεολαία και τη διανοητική ιδιοκτησία, το 2015 ποσοστό 52 % των νέων θεωρούσε σημαντική την ασφάλεια του διαδικτυακού τόπου κατά την πρόσβαση σε επιγραμμικό περιεχόμενο. Συνολικά 78 % των νέων δήλωσαν ότι θα ήταν ιδιαίτερα προσεκτικοί αν γνώριζαν ότι ο υπολογιστής ή η συσκευή τους κινδυνεύει να προσβληθεί από ιούς ή κακόβουλο λογισμικό. Συνολικά 84 % δήλωσαν ότι θα ήταν ιδιαίτερα προσεκτικοί αν γνώριζαν ότι κινδυνεύουν να κλαπούν τα στοιχεία της πιστωτικής τους κάρτας.

Στην έρευνα για την παρούσα μελέτη, το Γραφείο μάς ανέθεσε ένα τεχνικά πολύ δύσκολο καθήκον, να εντοπίσουμε και να τεκμηριώσουμε παραδείγματα κακόβουλου λογισμικού και PUP τα οποία θα μπορούσε να συναντήσει ο χρήστης του διαδικτύου στην προσπάθειά του να προσπελάσει δημοφιλείς πειρατικές κινηματογραφικές ταινίες, μουσική, βιντεοπαιχνίδια και τηλεοπτικά προγράμματα.

Στο πλαίσιο αυτό, επισημαίνεται ότι αποκλειστικός στόχος της έρευνας ήταν ο προσδιορισμός των τεχνικών χαρακτηριστικών του κακόβουλου λογισμικού και των PUP τα οποία συναντήσαμε στη διάρκεια της μελέτης και τα οποία θα μπορούσαν να συναντήσουν οι χρήστες του διαδικτύου που αναζητούν περιεχόμενο ύποπτο για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας. Τα δείγματα κακόβουλου λογισμικού και PUP που τεκμηριώθηκαν δεν είναι παρά μόνο ενδεικτικά και στόχος της μελέτης (και των αποτελεσμάτων της) δεν ήταν να εκτιμηθούν συνολικά οι πιθανότητες ή ο κίνδυνος τον οποίο διατρέχει ο χρήστης του διαδικτύου που αναζητά περιεχόμενο ύποπτο για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας να προσβληθεί από κακόβουλο λογισμικό ή PUP.

Η έρευνα διεξήχθη σε πολλαπλά στάδια, σε στενή συνεργασία με το Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο (EC3) της Ευρωπόλ.

Τα αποτελέσματα φανερώνουν ότι υπάρχουν πολλά και διάφορα κακόβουλα λογισμικά και PUP που απειλούν τον χρήστη του διαδικτύου ο οποίος αναζητά ύποπτο παράνομο περιεχόμενο. Τα περισσότερα από τα κακόβουλα λογισμικά ή PUP που τεκμηριώθηκαν μπορούν να χαρακτηριστούν «δούρειοι ίπποι» ή άλλο ανεπιθύμητο λογισμικό που μπορεί να αποκτήσει πρόσβαση στα προσωπικά δεδομένα των χρηστών του διαδικτύου χωρίς την άδειά τους. Τα παραδείγματα αυτά παρουσιάζουν ενδιαφέρον όχι μόνον για τους κατόχους δικαιωμάτων διανοητικής ιδιοκτησίας, αλλά και για τις αρχές επιβολής του νόμου και, επίσης, για τους καταναλωτές που ανησυχούν για την αυθαίρετη πρόσβαση στα προσωπικά τους δεδομένα.

Περίληψη

Στην παρούσα μελέτη γίνεται μια επισκόπηση των πιο πρόσφατων παραδειγμάτων κακόβουλου λογισμικού και δυνητικά ανεπιθύμητων προγραμμάτων (PUP) τα οποία βρέθηκαν σε διαδικτυακούς τόπους ύποπτους για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας. Τα προγράμματα αυτά χρησιμοποιούν παραπλανητικές τεχνικές και κοινωνική μηχανική —όπως κενές εφαρμογές εγκατάστασης παιχνιδιών ή φαινομενικά «χρήσιμο» λογισμικό— για να αποσπάσουν δολίως από τους τελικούς χρήστες ευαίσθητα δεδομένα τους.

Στόχος της παρούσας μελέτης είναι να ανακαλύψει και να τεκμηριώσει το κακόβουλο ή κατά τα λοιπά ανεπιθύμητο λογισμικό που διασπείρεται από επιλεγμένους διαδικτυακούς τόπους ύποπτους για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας και να κατηγοριοποιήσει τα ευρεθέντα δείγματα σύμφωνα με τις ποικίλες ταξινομήσεις κακόβουλου λογισμικού. Στο πλαίσιο αυτό, επισημαίνεται ότι αποκλειστικός στόχος της μελέτης ήταν ο καθορισμός των τεχνικών χαρακτηριστικών του κακόβουλου λογισμικού και των PUP τα οποία συναντήσαμε στη διάρκεια της έρευνας και τα οποία θα μπορούσαν να συναντήσουν οι χρήστες του διαδικτύου που αναζητούν περιεχόμενο ύποπτο για παραβίαση των δικαιωμάτων διανοητικής ιδιοκτησίας. Τα δείγματα κακόβουλου λογισμικού και PUP που τεκμηριώθηκαν δεν είναι παρά μόνο ενδεικτικά και στόχος της έρευνας (και των αποτελεσμάτων της) δεν ήταν να εκτιμηθούν συνολικά οι πιθανότητες ή ο κίνδυνος τον οποίο διατρέχει ο χρήστης του διαδικτύου που αναζητά περιεχόμενο ύποπτο για παραβίαση των δικαιωμάτων διανοητικής ιδιοκτησίας να προσβληθεί από κακόβουλο λογισμικό ή PUP. Για τους σκοπούς της παρούσας μελέτης, τα τηλεοπτικά προγράμματα, οι κινηματογραφικές ταινίες, η μουσική και τα βιντεοπαιχνίδια θεωρούνται περιεχόμενο του οποίου τα δικαιώματα διανοητικής ιδιοκτησίας προστατεύονται.

Πορίσματα της μελέτης

Το ύποπτο παράνομο περιεχόμενο συνιστά σημαντική παραβίαση των δικαιωμάτων διανοητικής ιδιοκτησίας. Υπάρχουν κάποιοι διαδικτυακοί τόποι που διαθέτουν δημόσια περιεχόμενο του είδους αυτού, ενίοτε ακόμη και δωρεάν, χωρίς εγγραφή. Παράλληλα με αυτό το περιεχόμενο, οι διαδικτυακοί τόποι συνήθως διανέμουν διαφόρων ειδών κακόβουλο λογισμικό και PUP, δελεάζοντας τους χρήστες να κατεβάσουν και να τρέξουν τα εν λόγω αρχεία. Στη διάρκεια του εντοπισμού των διαδικτυακών τόπων, με βάση την κατάταξη Alexa Top 500, πέρα από την προσομοίωση των αναζητήσεων του μέσου χρήστη σε γνωστές μηχανές αναζήτησης, όπως οι Google, Yahoo και Bing, διαπιστώθηκε ότι το σύνολο των διαδικτυακών τόπων είχε μεταβληθεί μεταξύ των δύο γύρων αναζήτησης. Η μεταβολή οφείλεται κατά πάσα πιθανότητα στις προσπάθειες των μηχανών αναζήτησης να διαγράψουν συνδέσμους προς διαδικτυακούς τόπους ύποπτους για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας, ενώ συνεχίζουν να εμφανίζονται νέοι ύποπτοι διαδικτυακοί τόποι. Όσον αφορά τους διαδικτυακούς τόπους που εντοπίστηκαν, ένα ενδιαφέρον εύρημα σχετίζεται με το γεγονός ότι η συντριπτική πλειονότητα των διαδικτυακών τόπων φιλοξενούνται στις ΗΠΑ ή έχουν ονομασία τομέα που συνδέεται με φιλοξενία στις ΗΠΑ. Αντίθετα, ελάχιστοι βρίσκονται σε διακομιστές εντός της ΕΕ. Εξάλλου, τα .com και .net είναι οι συχνότερες ονομασίες τομέα ανωτάτου επιπέδου που χρησιμοποιούνται από διαδικτυακούς τόπους ύποπτους για παραβίαση των δικαιωμάτων διανοητικής ιδιοκτησίας. Αυτό μπορεί να οφείλεται στο γεγονός ότι, σε αντίθεση με τους εθνικούς τομείς, αυτοί ενδέχεται να μην απαιτούν ταυτοποίηση του χρήστη με διαβατήριο ή άλλα έγγραφα αποδεικτικά της ταυτότητας. Κατά μέσον όρο προστέθηκαν 20 % νέοι διαδικτυακοί τόποι, ενώ 20 % των παλιών διαδικτυακών τόπων διαγράφηκαν ανάμεσα στους δυο γύρους της έρευνας. Εξάλλου, σχεδόν 8 % των διαδικτυακών τόπων που εντοπίστηκαν και στους δύο γύρους χαρακτηρίζονταν κακόβουλοι από την πλατφόρμα VirusTotal. Με τη χρήση διαφόρων συστημάτων διαχείρισης περιεχομένου, είναι πλέον πανεύκολο να δημιουργηθεί ένας διαδικτυακός τόπος και να διανέμεται περιεχόμενο στους χρήστες, ακόμη και κακόβουλες εφαρμογές.

Πριν από τη συλλογή κακόβουλου λογισμικού, η παρούσα μελέτη προέβη σε έλεγχο βάσει εγγράφων των απειλών από κακόβουλο λογισμικό το 2017 και σε κατηγοριοποίηση των πιο πρόσφατων εφαρμογών. Αυτό το σώμα γνώσεων χρησιμοποιήθηκε για την περαιτέρω ανάλυση του κακόβουλου λογισμικού σύμφωνα με τις καθολικά αποδεκτές αρχές για τα είδη κακόβουλου λογισμικού και τις οικογένειές τους. Συνολικά συγκεντρώθηκαν 106 αρχεία και στους δύο γύρους συλλογής δεδομένων, τα οποία περιλαμβάνουν αρχεία που μεταφορτώθηκαν απευθείας από διαδικτυακούς τόπους ύποπτους για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας, αλλά και αρχεία που δημιουργήθηκαν κατά την εκτέλεση των μεταφορτωθέντων αρχείων. Στη διάρκεια της μελέτης ανακαλύφθηκαν διάφορα PUP, είτε επρόκειτο για «χρήσιμο» λογισμικό, για απομιμήσεις εφαρμογές εγκατάστασης παιχνιδιών ή πελάτες για πλατφόρμες βίντεο συνεχούς ροής. Το λογισμικό αυτό δεν απειλεί κατ' ανάγκη άμεσα το λογισμικό ή το υλισμικό του χρήστη. Ωστόσο, μέσα από τεχνάσματα κοινωνικής μηχανικής, ο χρήστης μπορεί να πειστεί να αποκαλύψει ευαίσθητα προσωπικά δεδομένα ή στοιχεία καρτών πληρωμών. Εξάλλου, μπορεί να διαρρεύσουν πληροφορίες για τον ίδιο τον υπολογιστή προς τρίτους χωρίς τη ρητή συγκατάθεση του χρήστη.

Αρχικά, το κακόβουλο λογισμικό που συλλέχθηκε αναλύθηκε με χρήση εργαλείων ανοιχτού κώδικα προκειμένου να κατανοηθεί η εσωτερική λογική του, να εντοπιστούν πιθανές κακόβουλες δραστηριότητες και να αξιολογηθεί η σημασία τους για την παρούσα μελέτη σχετικά με το κακόβουλο λογισμικό. Πέρα από την προκαταρκτική ανάλυση με χρήση εργαλείων ανοιχτού κώδικα, τα συλλεχθέντα δείγματα κακόβουλου λογισμικού αναλύθηκαν από την πλατφόρμα «Λύση Ανάλυσης Κακόβουλου Λογισμικού» (Europol Malware Analysis Solution, EMAS) της Ευρωπόλ. Το αποτέλεσμα ήταν να εντοπιστεί ένας μεγάλος αριθμός τεχνασμάτων και κακόβουλων δραστηριοτήτων. Οι αναφορές της EMAS περιλαμβάνουν εκτενή ανάλυση των αρχείων που χρησιμοποιούν τέσσερις εκδόσεις των MS Windows, στην οποία καταγράφονται πλήρως για περαιτέρω ανάλυση η κίνηση του δικτύου, οι κλήσεις λειτουργιών και οι δραστηριότητες του δίσκου. Επιπλέον, η πλατφόρμα αναδεικνύει κάθε ύποπτη δραστηριότητα που εντοπίζεται κατά τις ρουτίνες εκτέλεσης των αρχείων. Αφού αναλύθηκαν όλες οι αναφορές, καταγράφηκαν 35 είδη κακόβουλης δραστηριότητας από την EMAS και ομαδοποιήθηκαν σε 17 κατηγορίες κακόβουλων συμβάντων. Ξεκινούν από γενικές ανωμαλίες (όπως η έναρξη διεργασιών συστήματος ή η αναζήτηση διεργασιών στις μνήμες) και φθάνουν έως αδιαμφισβήτητα κακόβουλες ενέργειες όπως η καταγραφή πληκτρολόγησης (keylogger), η πρόσβαση με προνόμια υπερχρήστη (rootkit) και η παρεμβολή στην κίνηση του δικτύου (network traffic tampering).

Γενικά, τα δυαδικά δείγματα κακόβουλου λογισμικού και PUP που συγκεντρώθηκαν αποκάλυψαν μικρό αριθμό διαφορετικών γενικών επιχειρηματικών μοντέλων: «χρήσιμα» προγράμματα που δήθεν καθαρίζουν παλιά αρχεία σε υπολογιστή χρήστη που έχει πληρώσει συνδρομή· προσομοιωτές εφαρμογών εγκατάστασης παιχνιδιών που ζητούν τα προσωπικά δεδομένα του χρήστη· δωρεάν προγράμματα που προσφέρουν πρόσβαση σε πλατφόρμες διανομής πειρατικού περιεχομένου, π.χ. μέσω ιχνηλάτη BitTorrent. Οι δύο γύροι εντοπισμού διαδικτυακών τόπων και συλλογής κακόβουλου λογισμικού απέδωσαν πολλά υποσχόμενα αποτελέσματα όσον αφορά την κατανόηση των μεθόδων διασποράς κακόβουλου λογισμικού και της κοινωνικής μηχανικής για την απόσπαση ευαίσθητων και ταυτοποιήσιμων προσωπικών δεδομένων. Εξάλλου, είναι εμφανής η αυξημένη δημοφιλία των κινητών συσκευών τα τελευταία χρόνια, λαμβάνοντας υπόψη το πλήθος των PUP για το λειτουργικό σύστημα Android που διατίθενται μέσα από τις πλατφόρμες οι οποίες είναι ύποπτες για διανομή παράνομου περιεχομένου. Από τη συσχέτιση των αναλύσεων προκύπτει το συμπέρασμα ότι το τοπίο των απειλών όσον αφορά το κακόβουλο λογισμικό που διανέμεται μέσα από διαδικτυακούς τόπους που παραβιάζουν δικαιώματα διανοητικής ιδιοκτησίας είναι πολύ πιο περίπλοκο απ' ό,τι θα νόμιζε κανείς με την πρώτη ματιά. Στα λογισμικά που ανακαλύφθηκαν, κάποια προγράμματα μπορούν να χαρακτηριστούν επιπλέον ως δούρειοι ίπποι (Trojan), διαφημιστικά (adware), κερκόπορτες (backdoor) ή πράκτορες (agent). Το τοπίο περιπλέκεται περαιτέρω από το γεγονός ότι βρέθηκαν επίσης πολλές ειδικές οικογένειες κακόβουλων λογισμικών, όπως το WisdomEyes, το DealPly και το FileRepMalware. Εξάλλου, αυτή η κατηγοριοποίηση ισχύει εν πολλοίς και για την πλατφόρμα Android, όχι μόνον για τα Microsoft Windows. Οι απειλές για τα δεδομένα των χρηστών καλύπτουν ένα ευρύ φάσμα, όχι μόνο την κλοπή ευαίσθητων ή προσωπικών δεδομένων, πληροφοριών για τη σύνθεση του υλισμικού του υπολογιστή ή τροποποίηση της κίνησης δικτύου. Ως εκ τούτου, ακόμη κι αν το εντοπισθέν λογισμικό είναι PUP, μπορεί να επηρεάσει τους χρήστες, ιδίως αν πρόκειται για τον

μέσο χρήστη ο οποίος μπορεί να μην έχει πλήρη επίγνωση των στοιχειωδών πρακτικών και μέτρων ασφαλείας στο διαδίκτυο.

Παράδειγμα των ευρημάτων της μελέτης παρατίθεται στη συνέχεια.

Διαδικτυακός τόπος 03	**Διαδικτυακός τόπος 09**	
Ο διαδικτυακός τόπος παραπλανεί τους χρήστες ώστε να χρησιμοποιήσουν μια εφαρμογή απομίμηση εγκατάστασης παιχνιδιού. Η όλη διαδικασία απόσπασης των ευαίσθητων δεδομένων του χρήστη έχει αλλάξει ανάμεσα στον πρώτο και τον δεύτερο γύρο συλλογής κακόβουλου λογισμικού. Ο χρήστης της υπηρεσίας αυτής κατεβάζει ένα αρχείο με περιεχόμενο δήθεν αρχεία που σχετίζονται με παιχνίδια και όχι ένα καθαρά δυαδικό εκτελέσιμο αρχείο που ανιχνεύεται από οποιοδήποτε αντιική εφαρμογή ως κακόβουλο. Το κρυπτογραφημένο αρχείο παρέχει πρόσβαση μόνο στα ονόματα των αρχείων και όχι στο ουσιαστικό περιεχόμενό τους.	Ο διαδικτυακός τόπος παρέχει πρόσβαση σε διαθέσιμα περιεχόμενα βίντεο κάθε είδους μέσα από ανιχνευτές torrent με τη βοήθεια λογισμικού. Το λογισμικό αυτό απαιτεί λιγότερες ενέργειες του χρήστη σε σύγκριση με άλλους ανιχνευτές BitTorrent. Αρκούν μερικά κλικ για να μεταφορτωθεί περιεχόμενο από άγνωστες πηγές, ενώ ο χρήστης δεν είναι προστατευμένος ούτε έχει τον έλεγχο του περιεχομένου που μεταφορτώνεται.	(Android) Ο διαδικτυακός τόπος παρέχει πρόσβαση σε ευρύ φάσμα δωρεάν εφαρμογών για κινητές συσκευές χωρίς εγγραφή. Μια εφαρμογή παρέχει απεριόριστη πρόσβαση σε συνεχή ροή τηλεοπτικών προγραμμάτων και κινηματογραφικών ταινιών. Ο χρήστης δεν καλείται ρητά να δώσει ευαίσθητα δεδομένα ή στοιχεία καρτών πληρωμών για να αγοράσει πρόσβαση σε βίντεο των οποίων τα δικαιώματα προστατεύονται. Ωστόσο, πρέπει να απενεργοποιήσει ρυθμίσεις ασφαλείας ώστε να επιτρέψει την εγκατάσταση εφαρμογών οι οποίες δεν προσομοιάζουν σε αυτές της επίσημης αγοράς εφαρμογών.

Μεθοδολογία

Για τη διεξαγωγή της έρευνας υιοθετήθηκε μια άρτια μεθοδολογία όσον αφορά αφενός την επιλογή των τίτλων και των διαδικτυακών τόπων και, αφετέρου, το τεχνικά δύσκολο εγχείρημα του εντοπισμού και της τεκμηρίωσης των ευρεθέντων δειγμάτων κακόβουλου λογισμικού και PUP. Ακολουθεί σύντομη επισκόπηση της μεθοδολογίας:

1. Στο στάδιο Ι της έρευνας του UNICRI, σε συνεργασία με το Ευρωπαϊκό Παρατηρητήριο παραβίασης των δικαιωμάτων διανοητικής ιδιοκτησίας («Παρατηρητήριο»), συγκροτήθηκε μια υποστηρικτική ομάδα εμπειρογνωμόνων για να παράσχει συμβουλές σχετικά με τη μεθοδολογία της έρευνας, την επιλογή των διαδικτυακών τόπων που χρησιμοποιήθηκαν για την ανάλυση και την αποτίμηση της έρευνας σε κάθε στάδιο της υλοποίησης του έργου. Στην υποστηρικτική ομάδα εμπειρογνωμόνων συμμετείχαν εκπρόσωποι των μελών του Παρατηρητηρίου, των οργανώσεων κατόχων δικαιωμάτων, ακαδημαϊκοί, εκπρόσωποι των διωκτικών αρχών και των οργανισμών της ΕΕ.

2. Παράλληλα, έγινε η επιλογή της ερευνητικής ομάδας. Στο πλαίσιο της παρούσας έκθεσης, δεν ήταν τεχνικά εφικτό [1] να ερευνηθούν όλα τα κράτη μέλη της ΕΕ. Για τον λόγο αυτό, στο στάδιο ΙΙ επιλέχθηκε ένα τυχαίο δείγμα 10 χωρών από τα 28 κράτη μέλη της ΕΕ.

[1] Ο επιλεγείς αριθμός χωρών θα είχε άμεσο αντίκτυπο (αυξητικό) στον αριθμό των επιλεγέντων διαδικτυακών τόπων ύποπτων για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας, καθώς και στον αντίστοιχο αριθμό δυαδικών αρχείων

3. Στο στάδιο III, εντοπίστηκαν δημοφιλείς κινηματογραφικές ταινίες, τηλεοπτικά προγράμματα, τραγούδια και βιντεοπαιχνίδια. Για τον ορισμό της δημοφιλίας λήφθηκε υπόψη η παγκόσμια δημοφιλία, αλλά και η δημοφιλία σε μία ή περισσότερες από τις 10 χώρες του δείγματος κατά την έναρξη της περιόδου συλλογής δεδομένων, στις 23 Ιουνίου 2017. Στα επόμενα στάδια της μελέτης, αυτοί οι δειγματοληπτικοί τίτλοι χρησιμοποιήθηκαν συστηματικά για τις επιγραμμικές αναζητήσεις στον παγκόσμιο ιστό ώστε να εντοπιστούν παράνομοι διαδικτυακοί τόποι και εφαρμογές για κινητές συσκευές. Κάθε τίτλος πληρούσε τουλάχιστον δύο από τα παρακάτω κριτήρια:

   - δημοφιλής κατά τον χρόνο συλλογής δεδομένων στα κράτη μέλη της ΕΕ
   - δημοφιλής κατά τον χρόνο συλλογής δεδομένων σε παγκόσμια κλίμακα
   - δημοφιλής ανέκαθεν σε παγκόσμια κλίμακα και
   - υπαγόμενος στην κατηγορία κινηματογραφική ταινία, τηλεοπτικό πρόγραμμα, τραγούδι ή βιντεοπαιχνίδι.

   Επιλέχθηκαν 5 τίτλοι κινηματογραφικών ταινιών, 5 τίτλοι τηλεοπτικών προγραμμάτων, 5 τίτλοι μουσικών κομματιών και 5 τίτλοι βιντεοπαιχνιδιών, με αποτέλεσμα να συγκεντρωθούν συνολικά 20 δειγματοληπτικοί τίτλοι. Οι πηγές που χρησιμοποιήθηκαν για να διαπιστωθεί η δημοφιλία κάθε τίτλου επιλέχθηκαν με μεγάλη προσοχή και συστηματικότητα, ώστε να διασφαλίζεται η ύπαρξη δεδομένων για όλα τα κράτη μέλη ή για την πλειονότητα αυτών.

4. Στο στάδιο IV εντοπίστηκαν διαδικτυακοί τόποι ύποπτοι για παροχή παράνομης πρόσβασης σε προστατευόμενο υλικό οι οποίοι είχαν μεγάλη επισκεψιμότητα παγκοσμίως και/ή στις 10 χώρες του δείγματος στις 26 Ιουνίου 2017 (πρώτος γύρος συλλογής κακόβουλου λογισμικού). Σε μεταγενέστερο στάδιο της μελέτης, οι εν λόγω διαδικτυακοί τόποι αναλύθηκαν για την παρουσία κακόβουλου λογισμικού και δυνητικά ανεπιθύμητων προγραμμάτων.

   Η μεθοδολογία για τον εντοπισμό των ύποπτων παράνομων διαδικτυακών τόπων αναπτύχθηκε με τη συμβολή της υποστηρικτικής ομάδας εμπειρογνωμόνων που συγκροτήθηκε στο στάδιο Ι, καθώς και με ανασκόπηση της υπάρχουσας βιβλιογραφίας από το UNICRI. Αναπτύχθηκε ειδικά για να δημιουργηθεί ένα δείγμα διαδικτυακών τόπων οι οποίοι:

   - είναι δημοφιλείς σε διάφορα κράτη μέλη της ΕΕ, γεγονός που διασφαλίζει ευρεία γεωγραφική κάλυψη
   - αντιπροσωπεύουν διαφόρων ειδών ύποπτους διαδικτυακούς τόπους για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας, όπως διαδικτυακούς τόπους συνεχούς ροής (streaming), διαδικτυακούς τόπους συνδέσμων (linking), διαδικτυακούς τόπους φιλοξενίας (hosting), διαδικτυακούς τόπους που προσφέρουν χώρο αποθήκευσης (cyberlockers) και διαδικτυακούς τόπους torrent
   - αντιπροσωπεύουν ευρύ φάσμα ύποπτων διαδικτυακών τόπων για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας που καλύπτουν κινηματογραφικές ταινίες, τηλεοπτικά προγράμματα, μουσική και βιντεοπαιχνίδια και
   - αντιπροσωπεύουν διαδικτυακούς τόπους τους οποίους πιθανότατα θα συναντήσει ο μέσος χρήστης του διαδικτύου στην απόπειρά του να προσπελάσει ύποπτο παράνομο υλικό.

   Η επιλογή των ύποπτων για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας διαδικτυακών τόπων έγινε σε πέντε βήματα. Τα τρία πρώτα σχεδιάστηκαν έτσι ώστε να εντοπιστούν οι πιο δημοφιλείς ύποπτοι παράνομοι διαδικτυακοί τόποι στα κράτη μέλη της ΕΕ. Η μέθοδος ήταν η απομίμηση των σεναρίων βάσει των οποίων ο μέσος χρήστης θα μπορούσε να αναζητήσει κάποιον ύποπτο παράνομο διαδικτυακό τόπο χωρίς να προσδιορίσει, π.χ., τον τίτλο ταινίας ή τραγουδιού. Τα δύο τελευταία σχεδιάστηκαν έτσι ώστε να εντοπίζονται οι ύποπτοι παράνομοι

προς ανάλυση. Για τον λόγο αυτό, αποφασίστηκε επικέντρωση μόνο σε ένα δείγμα χωρών ώστε να υλοποιηθεί επιτυχώς το πρακτικό σκέλος της μελέτης εντός συγκεκριμένου χρονοδιαγράμματος.

διαδικτυακοί τόποι τους οποίους θα μπορούσε να συναντήσει ο μέσος χρήστης κατά την αναζήτηση τρόπων να μεταφορτώσει συγκεκριμένο δημοφιλή τίτλο χωρίς να προσδιορίζει διαδικτυακό τόπο. Αυτό ήταν ιδιαίτερα σημαντικό, δεδομένου ότι υπάρχουν ύποπτοι κακόβουλοι διαδικτυακοί τόποι που αλλοιώνουν τα αποτελέσματα της αναζήτησης και εκμεταλλεύονται τα περιζήτητα θέματα μέσα από τη βελτιστοποίηση των μηχανών αναζήτησης. Οι δύο αυτές προσεγγίσεις, από κοινού, κάλυπταν τον τρόπο με τον οποίο ο μέσος χρήστης του διαδικτύου θα προσπαθούσε να βρει επιγραμμικά υλικό που παραβιάζει δικαιώματα διανοητικής ιδιοκτησίας.

Έμφαση δόθηκε στην ταυτόχρονη ανάλυση κακόβουλου λογισμικού και PUP ειδικά για εφαρμογές σε κινητές συσκευές, όπως έξυπνα τηλέφωνα και ταμπλέτες, ως μια από τις βασικές αναδυόμενες απειλές του εγκλήματος στον κυβερνοχώρο. Η ανάλυση περιορίστηκε σε συσκευές Android λόγω των ενδείξεων στην υπάρχουσα βιβλιογραφία για εντονότερη ύπαρξη κακόβουλου λογισμικού σε καταστήματα αγοράς εφαρμογών Android (π.χ. Google Play) απ' ό,τι στο κατάστημα Apple iTunes. Η μεθοδολογία αναπτύχθηκε έτσι ώστε να δημιουργηθεί ένα δείγμα εφαρμογών για κινητές συσκευές οι οποίες:

- είναι δημοφιλείς κατά τον χρόνο συλλογής των δεδομένων σε παγκόσμια κλίμακα
- αντιπροσωπεύουν διαφόρων ειδών εφαρμογές (περιλαμβανομένων εφαρμογών συνεχούς ροής, torrent και φιλοξενίας)
- περιέχουν ή παρέχουν πρόσβαση σε ποικίλο περιεχόμενο ύποπτο για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας (περιλαμβανομένων ταινιών, τηλεοπτικών τίτλων, μουσικής και παιχνιδιών για κινητές συσκευές) και
- αντιπροσωπεύουν αυτό που θα συναντήσει ο μέσος χρήστης κινητής συσκευής που προσπαθεί να μεταφορτώσει ή να χρησιμοποιήσει μια εφαρμογή που δίνει πρόσβαση σε ύποπτο προστατευόμενο περιεχόμενο.

5. Το στάδιο V συνίστατο σε συλλογή κακόβουλου λογισμικού και PUP, πέραν των εφαρμογών για κινητές συσκευές στους εντοπισθέντες διαδικτυακούς τόπους, προκειμένου να εξετασθούν και να κατηγοριοποιηθούν δεόντως σε μεταγενέστερο στάδιο. Το στάδιο της συλλογής δεδομένων περιλάμβανε δύο γύρους συλλογής κακόβουλου λογισμικού και ανάλυσης που διενεργήθηκαν στη διάρκεια του καλοκαιριού του 2017. Ο πρώτος γύρος συλλογής κακόβουλου λογισμικού κατέληξε σε 1 054 μοναδικές ονομασίες τομέα, ενώ ο δεύτερος γύρος απέφερε 1 057 μοναδικές ονομασίες τομέα στα 10 επιλεγμένα κράτη μέλη της ΕΕ. Η συλλογή του κακόβουλου λογισμικού έγινε με μη αυτοματοποιημένο και με αυτοματοποιημένο τρόπο, προκειμένου να προσομοιωθεί η εμπειρία του μέσου χρήστη.

Μη αυτοματοποιημένη συλλογή. Βάσει της μεθόδου αυτής, οι τομείς που είχαν εντοπιστεί στο προηγούμενο στάδιο ελέγχθηκαν με μη αυτοματοποιημένο τρόπο. Με τον τρόπο αυτό ο εμπειρογνώμονας μπορούσε να προσομοιώσει την εμπειρία του μέσου χρήστη του διαδικτύου, κάνοντας κλικ σε διαφημίσεις και αλληλεπιδρώντας με διαδικτυακούς τόπους που απαιτούσαν από τον χρήστη να κάνει κάποια ενέργεια.

Αυτοματοποιημένη συλλογή. Η μέθοδος αυτή χρησιμοποιούσε έναν αυτοματοποιημένο web crawler (πρόγραμμα ανίχνευσης ιστού) που είχε σχεδιαστεί από έναν εμπειρογνώμονα για να ακολουθεί όλους τους διαθέσιμους συνδέσμους σε διαδικτυακό τόπο ύποπτο για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας. Καταρχάς, σε κάθε διαδικτυακό τόπο ο crawler αρχικά συνέλεγε πληροφορίες από τους συνδέσμους στην κεντρική σελίδα. Στη συνέχεια ακολουθούσε καθέναν από τους συνδέσμους αυτούς προς τους δευτερεύοντες διαδικτυακούς τόπους. Στο τρίτο στάδιο, ο crawler ακολουθούσε καθέναν από τους συνδέσμους προς τριτεύοντες διαδικτυακούς τόπους. Σε κάθε βήμα, ο crawler ανακτούσε δυαδικά αρχεία τα οποία θα μπορούσαν να παρουσιάζουν ενδιαφέρον για τη μεταγενέστερη μη αυτοματοποιημένη ανάλυση, περιλαμβανομένου δυνητικού ή ύποπτου κακόβουλου λογισμικού και δυνητικά ανεπιθύμητων προγραμμάτων. Η διαδικασία αυτή συνεχιζόταν έως και τους 1 000 συνδέσμους ανά διαδικτυακό τόπο.

6. Αφού συγκεντρώθηκαν τα δυαδικά αρχεία, αναλύθηκαν σε ασφαλές υπολογιστικό περιβάλλον για να γίνει κατανοητή η εσωτερική λειτουργικότητά τους και να κατηγοριοποιηθούν αναλόγως. Η προκαταρκτική ανάλυση διενεργήθηκε με χρήση εργαλείων ανοικτού κώδικα προκειμένου να συσχετιστούν τα ευρήματα με αναφορές απειλών στον κυβερνοχώρο. Τα συλλεγέντα δείγματα λογισμικού απεστάλησαν στη συνέχεια προς ανάλυση στην EMAS. Η ανάλυση της EMAS συγκρίθηκε με τα προκαταρκτικά αποτελέσματα.

Επισκόπηση της μεθοδολογίας

Εντοπισθέντα δείγματα κακόβουλου λογισμικού και PUP

Στις 28 Ιουλίου 2017, στη διάρκεια του πρώτου γύρου συλλογής δεδομένων είχαν ελεγχθεί αυτομάτως 5 240 διαδικτυακοί τόποι (1 054 μοναδικοί), ενώ είχαν ανακτηθεί 617 συναφή αρχεία (μουσικής, βίντεο, αρχεία torrent και λογισμικού) συνολικού μεγέθους 47 GB. Το μη κατηγοριοποιημένο αυτό σύνολο αρχείων απαιτούσε περαιτέρω ανάλυση προκειμένου να διαπιστωθεί ποια από τα συλλεγέντα αρχεία ήταν συναφή για τη μελέτη. Τα δείγματα των παράνομων διαδικτυακών τόπων ήταν παρεμφερή και στις 10 χώρες του δείγματος για κάθε είδος μέσου (τηλεοπτικά προγράμματα, κινηματογραφικές ταινίες, μουσική και βιντεοπαιχνίδια). Έτσι, από τις χώρες του δείγματος επιλέχθηκε τυχαία το Βέλγιο και ελέγχθηκαν με μη αυτοματοποιημένο τρόπο όλοι οι εντοπισθέντες παράνομοι διαδικτυακοί τόποι του Βελγίου για την παρουσία κακόβουλου ή κατά τα λοιπά ανεπιθύμητου λογισμικού. Στις 10 Αυγούστου 2017, μετά τον δεύτερο γύρο συλλογής, είχαν συγκεντρωθεί αυτόματα συνολικά 3 665 αρχεία από διαδικτυακούς τόπους στο σύνολο των χωρών, συνολικού μεγέθους 167 GB. Ο συνολικός αριθμός μοναδικών URL που συγκεντρώθηκαν σε όλες τις χώρες ήταν 1 057 επί συνόλου 5 606 διαδικτυακών τόπων, αριθμός που ήταν ανέφικτο να ελεγχθεί στο σύνολό του με μη αυτοματοποιημένο τρόπο.

Μετά από προκαταρκτική ανάλυση των συγκεντρωθέντων αρχείων, εξήχθησαν 106 μοναδικά δυαδικά αρχεία για τα λειτουργικά συστήματα MS Windows, Android και Mac έπειτα από τους δύο γύρους συλλογής κακόβουλου λογισμικού. Ειδικότερα, επιλέχθηκαν 41 αρχεία στον πρώτο γύρο

και 65 στον δεύτερο —συγκεκριμένα 2 για Mac, 15 για Android και 89 για MS Windows. Από τα αρχεία αυτά, 21 μπορούν να θεωρηθούν γνωστά κακόβουλα προγράμματα, χαρακτηρισμένα από πλήθος πωλητών αντιικών εφαρμογών της πλατφόρμας VirusTotal. Μεταξύ αυτών συγκαταλέγονται αρχεία που έχουν μεταφορτωθεί απευθείας από διαδικτυακούς τόπους που είναι ύποπτοι για παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας, αλλά και αρχεία που δημιουργούνται κατά την εκτέλεση των αρχείων που έχουν μεταφορτωθεί. Στη συνέχεια, τα συλλεχθέντα δείγματα λογισμικού αναλύθηκαν σε περιβάλλον μη εξουσιοδοτημένων εφαρμογών (sandbox environment) και παραδόθηκαν στην EMAS για πιο εμπεριστατωμένη ανάλυση πιθανών κακόβουλων ενεργειών. Συνολικά, από όλα τα δυαδικά αρχεία αποκαλύφθηκαν 821 διακριτά κακόβουλα συμβάντα σε 4 αναφορές της EMAS (Windows 7 SP1, Windows7 SP1 64-bit, Windows 10 64-bit, Windows XP SP3). Κάποιες από τις αναφορές δεν είχαν καμία ύποπτη δραστηριότητα, ενώ κάποιες είχαν έως και 10 ήδη γνωστές κακόβουλες δραστηριότητες. Στη διάρκεια του τελευταίου σταδίου της μελέτης, έγινε συσχέτιση των αποτελεσμάτων της προκαταρκτικής ανάλυσης και των αναφορών της EMAS. Η ποσοτική σύνοψη των αποτελεσμάτων παρατίθεται στον παρακάτω πίνακα.

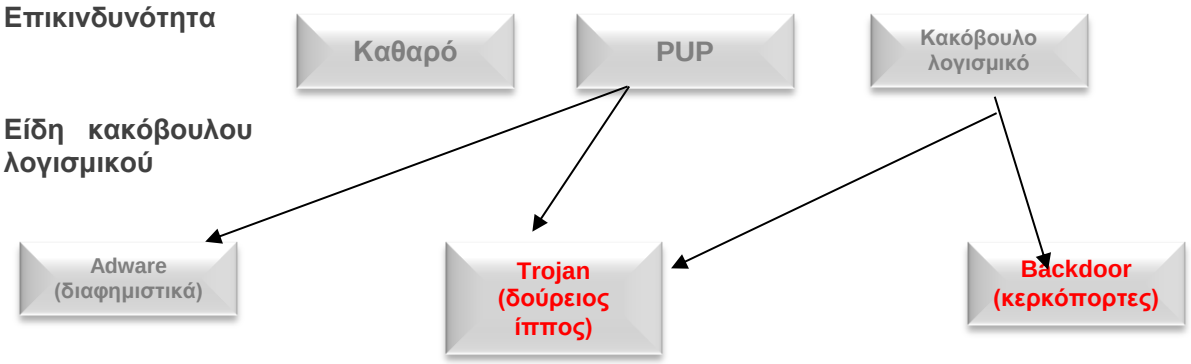
	Γύρος 1	**Γύρος 2**
Ημερομηνία	28 Ιουλίου 2017	10 Αυγούστου 2017
Διαδικτυακοί τόποι που εντοπίστηκαν σε 10 κράτη μέλη της ΕΕ	5 240	5 606
Μοναδικοί διαδικτυακοί τόποι	1 054	1 057
Συναφή αρχεία	617	3 665 [2]
Μέγεθος συναφών αρχείων, GB	47	167
Παράδοση στην EMAS		
Android	3	12
Mac OS	2	–
MS Windows	36	53
Συνολικό μέγεθος, bytes	175 600 117	522 991 095

Λύση Ανάλυσης Κακόβουλου Λογισμικού (EMAS) της Ευρωπόλ

Η «Λύση Ανάλυσης Κακόβουλου Λογισμικού» της Ευρωπόλ (EMAS) είναι μια δυναμική, αυτοματοποιημένη λύση ανάλυσης κακόβουλου λογισμικού που παρέχεται από την Ευρωπόλ στα κράτη μέλη. Η EMAS παρέχει τη δυνατότητα δημιουργίας εκθέσεων ανάλυσης, αλλά το πιο επαναστατικό της χαρακτηριστικό είναι ότι παράγει εκθέσεις πληροφοριών για την αστυνομία. Οι αυτοματοποιημένες διασταυρώσεις μπορούν να καταδείξουν τη σύνδεση μεταξύ επιθέσεων που έγιναν σε διάφορες χώρες με το ίδιο κακόβουλο λογισμικό ή από την ίδια εγκληματική οργάνωση που δρα πίσω από τη συγκεκριμένη οικογένεια κακόβουλου λογισμικού, συνδεόμενες με τους ίδιους τομείς και σχετιζόμενες με διάφορες έρευνες εντός και εκτός ΕΕ. Το 2015 η EMAS αυτοματοποιήθηκε πλήρως ώστε να επιτρέπει την άμεση πρόσβαση σε διωκτικές αρχές με τις οποίες η Ευρωπόλ έχει συνάψει επιχειρησιακές συμφωνίες. Το 2015 αναλύθηκαν 525 108 αρχεία στην EMAS, εκ των οποίων 356 863 χαρακτηρίστηκαν κακόβουλα.

[2] Η αριθμητική διαφορά μεταξύ πρώτου και δεύτερου γύρου ερμηνεύεται από το γεγονός ότι, στη διάρκεια του δεύτερου γύρου αυτοματοποιημένης συλλογής, υπήρχαν διαδικτυακοί τόποι που δημοσίευαν πολλαπλά σύνολα αρχείων σε κάθε ιστοσελίδα τους.

Όπως φαίνεται στο διάγραμμα που ακολουθεί, τα συλλεγέντα δυαδικά αρχεία γενικά κατηγοριοποιούνται σύμφωνα με την επικινδυνότητά τους, ως ακίνδυνα (αρχεία που δεν εγκυμονούν κανέναν κίνδυνο), ως PUP ή ως επικίνδυνο κακόβουλο λογισμικό. Εξάλλου δεν αποκαλύφθηκαν PUP μόνο για το λειτουργικό σύστημα Microsoft Windows, αλλά και για το Android και για το Mac, γεγονός που σημαίνει ότι όσοι αναπτύσσουν κακόβουλο λογισμικό προσπαθούν να επηρεάσουν τον μέγιστο δυνατό αριθμό χρηστών χρησιμοποιώντας διάφορες πλατφόρμες. Τα PUP και το κακόβουλο λογισμικό μπορούν να διαφοροποιηθούν περαιτέρω, ως «δούρειοι ίπποι» (Trojan), διαφημιστικά (adware) ή κερκόπορτες (backdoor). Η πλειονότητα του εντοπισθέντος λογισμικού εμπίπτει στην κατηγορία PUP. Η λειτουργία των PUP σχετίζεται με ένα από τα ακόλουθα επιχειρηματικά μοντέλα: δήθεν εγκατάσταση παιχνιδιών για την οποία ζητούνται προσωπικά δεδομένα ή στοιχεία τραπεζικού λογαριασμού, μεταφόρτωση «χρήσιμων» προγραμμάτων που αναγκάζουν τους χρήστες να καταβάλουν συνδρομή ή εγκατάσταση δωρεάν προγραμμάτων για πρόσβαση σε πλατφόρμες που παραβιάζουν δικαιώματα διανοητικής ιδιοκτησίας. Οι εφαρμογές αυτές μπορεί να αποτελούν κίνδυνο για τα προσωπικά στοιχεία του χρήστη και τις ρυθμίσεις του υπολογιστή του. Μέσα από τεχνάσματα κοινωνικής μηχανικής, μπορεί να αποκαλυφθούν διαφόρων ειδών προσωπικά δεδομένα, όπως στοιχεία καρτών πληρωμών, πληροφορίες μέσω των οποίων μπορεί να ταυτοποιηθεί το πρόσωπο ή στοιχεία λογαριασμών στα μέσα κοινωνικής δικτύωσης. Στην έρευνα εντοπίστηκαν επίσης 15 εφαρμογές Android από τρίτους και, κατόπιν προκαταρκτικής ανάλυσης, προκύπτει το συμπέρασμα ότι οι εν λόγω εφαρμογές μπορεί να ενέχονται στη διανομή περιεχομένου που παραβιάζει δικαιώματα διανοητικής ιδιοκτησίας ή αποκαλύπτει προσωπικά δεδομένα.



Απειλές για τους τελικούς χρήστες

Στη διάρκεια των δύο γύρων εντοπισμού διαδικτυακών τόπων και ανάλυσης κακόβουλου λογισμικού, δεν βρέθηκε λογισμικό εκβίασης (λυτρισμικό). Γενικά, η πλειονότητα του συλλεχθέντος κακόβουλου λογισμικού μπορεί να χαρακτηριστεί «δούρειος ίππος», μπορεί δηλαδή να εμφανίζεται στους διαδικτυακούς τόπους ως άκακο, ευρέως διαδεδομένο ή δημοφιλές λογισμικό, ενώ στην πραγματικότητα μπορεί να κλέψει ή να αποκαλύψει προσωπικά δεδομένα. Ο άπειρος χρήστης μπορεί να επιδείξει μεγάλη εμπιστοσύνη στο λογισμικό και να μην παρατηρήσει τυχόν ανωμαλίες. Εξάλλου, η στατική ανάλυση και οι δυναμικές συμπεριφορικές παρατηρήσεις του εν λόγω λογισμικού μπορεί να μην αποκαλύπτουν πλήρως τη λειτουργικότητά του ελλείψει του πηγαίου κώδικα. Μετά από την προκαταρκτική ανάλυση του κακόβουλου λογισμικού, η ανάλυση της EMAS κατέδειξε πιο συγκεκριμένες κακόβουλες δραστηριότητες. Η εγκατάσταση του συγκεκριμένου λογισμικού σε υπολογιστή τελικού χρήστη μπορεί να έχει σημαντικές συνέπειες, προκαλώντας όχι μόνο οικονομική ζημία, αλλά και κλοπή προσωπικών δεδομένων και άλλους κινδύνους ανεπιθύμητης πρόσβασης και ελέγχου. Οι δραστηριότητες αυτές μπορεί να καταλήξουν σε συγκέντρωση προσωπικών δεδομένων και σε μετάδοση αυτών σε τρίτους σε κρυπτογραφημένη ή μη μορφή. Τα εν λόγω δεδομένα μπορεί να είναι, για παράδειγμα, στοιχεία τραπεζικών λογαριασμών από την εφαρμογή περιήγησης, στοιχεία ρυθμίσεων του υλισμικού/λογισμικού του υπολογιστή ή κατ' ουσίαν οτιδήποτε πληκτρολογείται στο πληκτρολόγιο.

ΕΝΤΟΠΙΣΜΟΣ ΚΑΙ ΑΝΑΛΥΣΗ ΤΟΥ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΣΕ ΕΠΙΛΕΓΜΕΝΟΥΣ ΔΙΑΔΙΚΤΥΑΚΟΥΣ ΤΟΠΟΥΣ ΥΠΟΠΤΟΥΣ ΓΙΑ ΠΑΡΑΒΙΑΣΗ ΔΙΚΑΙΩΜΑΤΩΝ ΔΙΑΝΟΗΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

ΠΕΡΙΛΗΨΗ

Σεπτέμβριος 2018