Ασφάλεια Πληροφοριακών Συστημάτων
Εργασία Εαρινού Εξαμήνου 2022

"Τοπικότητα των Κυβερνοαπειλών: Ιομορφικό Λογισμικό"

Ευγένιος Γκρίτσης ΑΜ 3190045 - Γεώργιος Σύρος ΑΜ 3190193

Περιεχόμενα

Προς το διοικητικό συμβούλιο του ΜΚΟ “DigTech”,

1. Εισαγωγή

Το παρόν έγγραφο αποτελεί έρευνα για το μείζον ζήτημα του ιομορφικού λογισμικού (malware) και αναφορά για το κοινωνικό, πολιτικό και νομικό πλαίσιο στις χώρες των Ηνωμένων Πολιτειών της Αμερικής (ΗΠΑ) και του Χονγκ-Κονγκ (ΧΚ). Ειδικότερα, ορίζονται τα μείζονα είδη απειλών και αναλύονται κάποια από τα σημαντικότερα περιστατικά κυβερνοεπιθέσεων με χρήση ιομορφικού λογισμικού, τονίζοντας την βαρύτητα και το εύρος της απειλής. Στη συνέχεια μελετώνται οι δυνατότητες και περιορισμοί για την αντιμετώπιση τους στις περιοχές που αναφέρθηκαν παραπάνω. Τέλος, με βάση όσων έχουν ειπωθεί, εξάγονται πολύτιμα συμπεράσματα που θα βοηθήσουν στην λήψη αποφάσεων για την υπό συζήτηση μελλοντική επέκταση των δραστηριοτήτων της εταιρείας στις ΗΠΑ και ΧΚ.

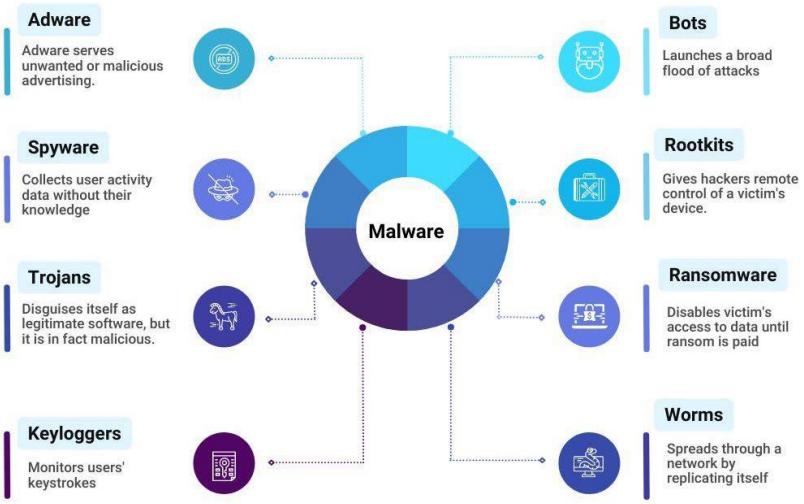
2. Η αόρατη απειλή: Ιομορφικό Λογισμικό.

2.1 Ορισμός και μορφές

Είναι ευρέως αποδεκτό ότι με την τεχνολογική πρόοδο των τελευταίων δύο δεκαετιών η κοινωνία άλλαξε και συνεχώς αλλάζει μορφή με την ολοένα αυξανόμενη «ψηφιοποίηση» του τρόπου ζωής. Η ραγδαία αλλαγή έχει επηρεάσει κάθε οντότητα και πιο συγκεκριμένα τις επιχειρήσεις. Από τον νέο ψηφιακό τρόπο λειτουργίας και δραστηριοποίησής τους προέκυψαν και προκύπτουν νέοι κίνδυνοι αστοχίας των υποδομών τους, με την άποψη ειδικών να συμφωνούν ότι «το σημαντικότερο πρόβλημα να αποτελεί το ιομορφικό λογισμικό, καθώς συνεχώς προκύπτουν νέες και πιο δύσκολα αντιμετωπίσιμες μορφές του» (Γκρίτζαλης, 2019).

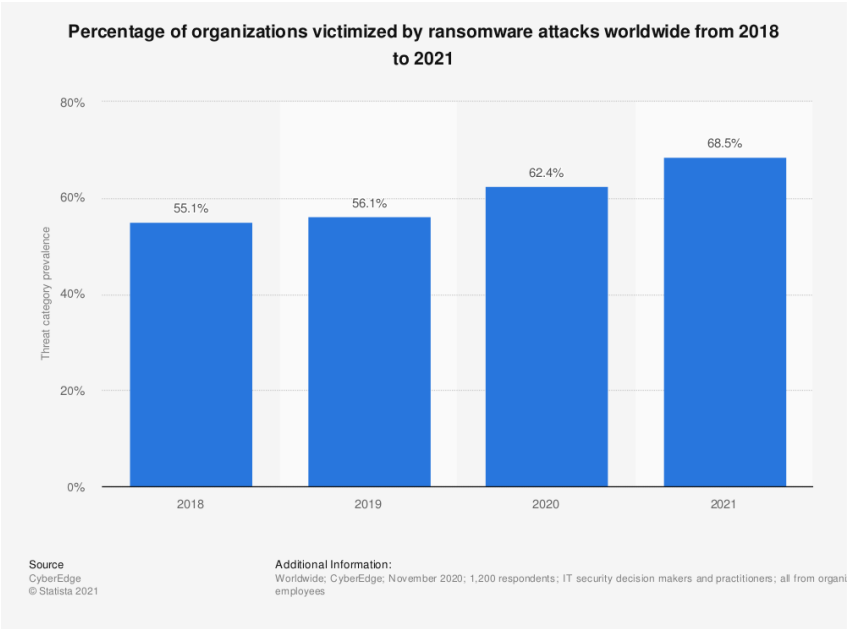
Για την κατανόηση της απειλής απαιτείται πρώτα καλή κατανόηση του τί ορίζεται ως «ιομορφικό λογισμικό». Αποφεύγοντας ορισμούς που απαιτούν ειδικές επιστημονικές γνώσεις στο πεδίο της Κυβερνοασφάλειας, με έναν πολύ διαισθητικό τρόπο, το κακόβουλο ιομορφικό λογισμικό ορίζεται ως λογισμικό που επιτίθεται επιβλαβώς σε άλλο λογισμικό, που ως *επιβλαβώς* παρατηρείται να σημαίνει αλλοίωση της επιθυμητής συμπεριφοράς (Simon Kramer, 2010). Κατά τους εμπειρογνώμονες (Jaikaran, 2021) υπάρχουν πολλοί τρόποι που ένα ιομορφικό λογισμικό μπορεί να προστεθεί σε ένα προϊόν λογισμικού, όπως για παράδειγμα από ένα USB flash drive («στικάκι») ή μέσω λήψης από το διαδίκτυο. Τα δεδομένα μπορούν να προσβληθούν παραβιάζοντας την ιδιωτικότητά τους (διακύβευση της εμπιστευτικότητας), να τροποποιηθούν (διακύβευση της ακεραιότητας), ή να διαγραφούν (διακύβευση της διαθεσιμότητας).

Έπειτα από την μαθηματική θεμελίωση της ιομορφής (Cohen, 1987), με την πάροδο του χρόνου οι αναλυτές κυβερνοασφάλειας έχουν ομαδοποιήσει το ιομορφικό λογισμικό βάσει της λειτουργικότητας του, με στόχο την ακριβέστερη μελέτη του. Από τις σημαντικότερες κατηγορίες ιομορφικού λογισμικού είναι το πρόγραμμα Ιός (Virus), ο Δούρειος Ίππος (Trojan) και ο Αναπαραγωγός (Worm).



Εικόνα 1: 8 πιο διαδεδομένα είδη malware [Πηγή: SECUREB4]

Παρατηρώντας τις τάσεις των τελευταίων ετών με κριτήριο τον βαθμό περιορισμού των δραστηριοτήτων ενός οργανισμού (δημόσιου ή ιδιωτικού) διακρίνονται δύο ειδικές κατηγορίες ιών: το Λυτρισμικό (Ransomware) και το Λογισμικό Κατασκοπείας (Spyware). Ειδικότερα, το Λυτρισμικό στοχεύει στην άρνηση πρόσβασης σε δεδομένα και πληροφοριακά συστήματα κρυπτογραφώντας τα αρχεία και μέρη τους, αποκλείοντας έτσι τους χρήστες από αυτά. Ο δράστης ωθεί το θύμα σε πληρωμή λύτρων, συνήθως με κρυπτονομίσματα, για την αποκρυπτογράφηση του συστήματος (Jaikaran, 2021). Ως επιπρόσθετο μέσο πίεσης, ο δράστης προειδοποιεί το θύμα πως έχει υποκλέψει τα δεδομένα του και απειλεί με την δημοσίευση τους. Σε αντίθεση με τα εμφανή αποτελέσματα μιας επίθεσης με την χρήση Λυτρισμικού, το λογισμικό κατασκοπείας βασίζεται στην μυστικότητα της επιχείρησης του. Αποτελεί ένα «Φάντασμα» (Stafford & Urbaczewski, 2004) το οποίο τρέχει στο παρασκήνιο χωρίς την γνώση και συγκατάθεση του ιδιοκτήτη του συστήματος. Στόχος του είναι η παρακολούθηση και αναφορά της δραστηριότητας των χρηστών του συστήματος σε κάποιον τρίτο.



Εικόνα 2: Ποσοστό οργανισμών που έχουν υπάρξει θύματα επιθέσεων με λυτρισμικό παγκοσμίως από το 2018 εως το 2021.

2.2 Διάσημα περιστατικά κυβερνοεπιθέσεων

Έκπληξη προκαλεί το γεγονός ότι «οι μεγαλύτεροι σε μέγεθος οργανισμοί μεριμνούν λιγότερο, παρότι αποτελούν πιο συχνά στόχο επίδοξων επιτιθέμενων και αντιμετωπίζουν μεγαλύτερο αριθμό περιστατικών ανασφάλειας ετησίως, με σημαντικά σοβαρότερες επιπτώσεις» (Γκρίτζαλης, 2019). Λαμβάνοντας υπόψιν το διαθέσιμο κεφάλαιο των οργανισμών του συγκεκριμένου βελληνεκούς, ακούγεται αδιανόητο. Όπως ερμηνεύτηκε από ειδικούς (Σπινέλλης, et al., 1999), αν και οι επενδύσεις των μικρών επιχειρήσεων σε τεχνολογίες πληροφορίας και επικοινωνιών είναι μικρές, η επικινδυνότητα που αντιμετωπίζουν είναι ίση η μεγαλύτερη αυτής των μεγάλων επιχειρήσεων. Αυτό πηγάζει από το γεγονός πως οι μικρές επιχειρήσεις δεν διαθέτουν τους πόρους που θα τους επιτρέψουν να ανακάμψουν από μια καταστροφή των πληροφοριακών τους υποδομών, σε αντίθεση με μεγάλες επιχειρήσεις που έχουν την δυνατότητα να αποδεσμεύσουν πόρους από άλλες δραστηριότητες τους.

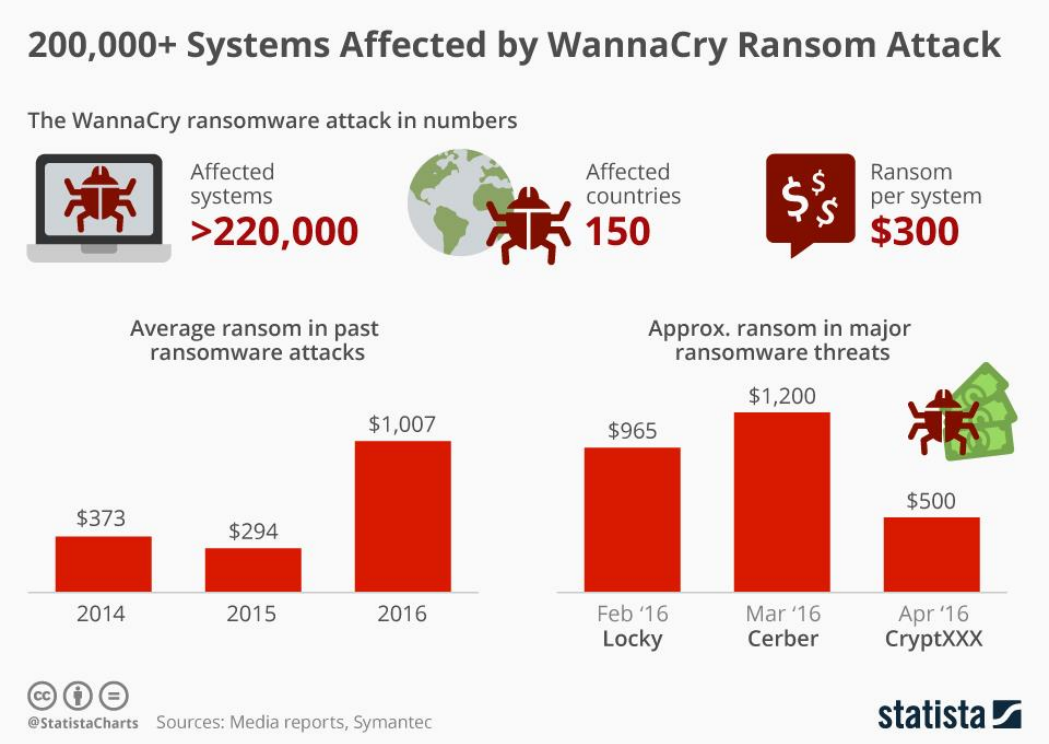
Για καλύτερη κατανόηση του εύρους της απειλής κυβερνοεπιθέσεων με την χρήση ιομορφικού λογισμικού θα ήταν αρμόζον να μελετηθούν εξέχοντα περιστατικά επιθέσεων σε παγιωμένους οργανισμούς παγκοσμίως.

Χαρακτηριστικό παράδειγμα κυβερνοεπίθεσης με καταστροφικές συνέπειες είναι η «πανδημία» του λυτρισμικού «WannaCry». Το συγκεκριμένο ιομορφικό λογισμικό εκμεταλλευόταν μια προηγουμένως άγνωστη στην κοινότητα ευπάθεια (“zero-day”) του λειτουργικού συστήματος Windows με κωδική ονομασία “Eternal Blue” το οποίο κλάπηκε από την National Security Agency (NSA) των ΗΠΑ.

Εικόνα 3: Παράθυρο προειδοποίησης λυτρισμικού WannaCry

Μια σειρά επιθέσεων έλαβε χώρα σε διάφορους οργανισμούς στον τομέα της υγείας, ασφάλειας, τηλεπικοινωνιών, πετρελαίου, αυτοκινητοβιομηχανίας, εκπαίδευσης και διαφήμισης. Το λυτρισμικό μόλυνε κατά εκτίμηση περίπου 230.000 υπολογιστές σε 150 χώρες σε χρονικό διάστημα μόλις μερικών ωρών (Malwarebytes, n.d.). Λόγω της πληθώρας των κυβερνητικών υπηρεσιών, πανεπιστημίων, οργανισμών υγείας και άλλων ιδιωτικών επιχειρήσεων που επλήγησαν από το WannaCry, το κόστος της ζημιάς σε συνδυασμό με το κόστος αποκατάστασης ήταν υπέρογκο. Η

εταιρεία κυβερνοασφάλειας Cyence εκτιμά το συνολικό κόστος των επιθέσεων μέχρι και 4 δισεκατομμύρια δολάρια (Berr, 2017).



Εικόνα 4: Σύνοψη επιθέσεων λυτρισμικού

Όσον αφορά κυβερνοεπιθέσεις με λογισμικό κατασκοπείας, αξιοσημείωτο περιστατικό αποτελεί το σκάνδαλο τηλεφωνικών υποκλοπών στην Ελλάδα κατά την περίοδο 2004-2005. Συγκεκριμένα, αφορούσε λογισμικό το οποίο είχε εγκατασταθεί στα συστήματα της εταιρείας τηλεπικοινωνιών Vodafone με σκοπό την κατασκοπεία και υποκλοπή συνομιλιών 106 αξιωματούχων της ελληνικής κυβέρνησης, συμπεριλαμβανομένου του Έλληνα πρωθυπουργού, και στρατιωτικής ηγεσίας (Brabant, 2006). Αναλυτές αναφέρουν πως η παρακολούθηση ξεκίνησε το καλοκαίρι του 2004 και διήρκησε έως και τον Μάρτιο του 2005 όταν εντοπίστηκε η παραβίαση των συστημάτων. Τα κίνητρα δεν είναι σαφή όμως αναλυτές αποδίδουν την κυβερνοεπίθεση -χωρίς να έχει επιβεβαιωθεί- σε αμερικανικές μυστικές υπηρεσίες. Ωστόσο, οι συνέπειες ήταν αισθητές τόσο από το εταιρικό αλλά και από το πολιτικό περιβάλλον. Η εταιρεία καταδικάστηκε υπεύθυνη για την ανικανότητα της να αποτρέψει την κυβερνοεπίθεση και κλήθηκε να πληρώσει πρόστιμο ύψους 76 εκατομμυρίων ευρώ. Παράλληλα, διακυβεύτηκε η φήμη και αξιοπιστία της ελληνικής κυβέρνησης με τεράστια ερωτήματα να παραμένουν αναπάντητα.

Οι δύο κυβερνοεπιθέσεις εξελέγησαν από ένα -πλέον- μη αριθμήσιμο σύνολο περιστατικών με σκοπό να υπογραμμιστεί η ικανότητα και ο ρόλος του ιομορφικού λογισμικού στην άμεση (WannaCry-Ransomware) και έμμεση (Vodafone Wiretapping-Spyware) πλήξη των δραστηριοτήτων ενός οργανισμού.

3. Δύση και Ανατολή: δυο κόσμοι αντίθετοι.

3.1 Εισαγωγή

«Αν ο χάκερ είχε ταυτοποιηθεί και τύχαινε να είναι Βραζιλιάνος πολίτης, θα μπορούσε να εξαναγκαστεί σε δίκη στις ΗΠΑ; Ίσως όχι. Αν ο χάκερ προσπαθούσε να αποφύγει την έκδοσή του, τί διέξοδο θα μπορούσαν να χρησιμοποιήσουν οι ΗΠΑ για να εξασφαλίσουν την σύλληψη του και καταδίκη εντός της δικαιοδοσίας τους; Η απάντηση είναι πολλή μικρή. Γιατί; Διότι ακόμα και εάν έγκυρο αμερικάνικο ένταλμα μπορούσε να εκδοθεί για τη σύλληψη του υπόπτου, εφόσον η Βραζιλία δεν διέθετε νόμους κυβερνοασφάλειας, θα ήταν αδύνατο να ικανοποιήσει το αίτημα έκδοσης (φαινόμενο γνωστό και ως "dual criminality"). Επομένως, στο προηγούμενο σενάριο ο δράστης δεν θα μπορούσε να καταστεί υπεύθυνος λόγω ελλείψεων στο διεθνή και εγχώριο νόμο. Παρόλο που δύναται να προκλήθηκαν ζημιές εκατομμυρίων δολαρίων -και ίσως και απώλεια ζωής- ο δράστης μπορεί να διαφύγει, ένα αποτέλεσμα που μπορεί να προκαλέσει διπλωματικό επεισόδιο μεταξύ δύο παραδοσιακά πολύ καλών συμμάχων».

Με αυτόν τον πολύ διαισθητικό τρόπο (Ghosh, 2001) παρουσιάζεται ο βαθμός πολυπλοκότητας και ευαισθησίας διεθνών περιστατικών κυβερνοεγκλημάτων. Στις υποενότητες που ακολουθούν σχολιάζεται το κοινωνικό, πολιτικό και νομικό πλαίσιο των ΗΠΑ και του Χονγκ-Κογνκ υποστηριζόμενο από γνώμες ειδικών αναλυτών, ακαδημαϊκών και εμπειρογνωμόνων.

3.2 Ηνωμένες Πολιτείες Αμερικής

Οι ΗΠΑ έχουν υπάρξει ιστορικά ένας από τους κύριους στόχους κυβερνοεπιθέσεων παγκοσμίως εξαιτίας του ενεργού ρόλου που διαδραματίζουν στις διεθνείς εξελίξεις. Ως εκ τούτου, η κυβέρνηση των ΗΠΑ έχει μεριμνήσει για την θέσπιση νομοθεσίας που αφορά την ασφάλεια στον κυβερνοχώρο. Είναι γεγονός ότι σε χρονικό διάστημα 30 ετών, τα κυβερνοεγκλήματα όντας αρχικά ανύπαρκτα, κάλυψαν κάθε είδος δραστηριότητας στο διαδίκτυο.

3.2.1 Το πρώτο βήμα

Η πρώτη σοβαρή προσπάθεια νομικής οριοθέτησης του συνεχώς τεχνολογικά αναπτυσσόμενου κυβερνοχώρου ήταν το "CFAA" (Computer Fraud & Abuse Act, 1986). Το Κογκρέσο μέσω αυτής της πράξης νομικού περιεχομένου απαγόρευσε την μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές «ομοσπονδιακού ενδιαφέροντος», θεσπίζοντας ρητά [παράγραφος 1030(a)(5)] παράνομη οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικό υπολογιστή και την πρόκληση αλλοίωσης ή καταστροφής πληροφορίας (National Association Of Criminal Defense Lawyers, 2020). Τα επόμενα χρόνια ακολούθησαν διάφορες τροπολογίες με στόχο την επικαιροποίηση και εμπλουτισμό του νόμου.

3.2.2 Η εξέλιξη

Ένα από τα πιο καθοριστικά γεγονότα της νεότερης ιστορίας των ΗΠΑ αποτέλεσε η τρομοκρατική επίθεση της 11ης Σεπτεμβρίου, η οποία λειτούργησε ως καταλύτης στην καθιέρωση ενός νομικού πλαισίου που επέφερε σημαντικές αλλαγές στην τότε νομοθεσία. Η πράξη νομικού περιεχομένου "USA PATRIOT" (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, γνωστό ως USAPA*) στόχευε στην δραματική ενίσχυση της εθνικής ασφάλειας των ΗΠΑ, ιδίως όσον αφορά την εγχώρια και ξένη τρομοκρατία. Γενικά, «η πράξη δημιουργεί νέους τρόπους με τους οποίους η κυβέρνηση των ΗΠΑ μπορεί να παρακολουθεί και να εξάγει προσωπικές πληροφορίες» (Nockleby, 2002) από πρόσωπα και οργανισμούς.

Αξιοσημείωτη, ωστόσο, για τον τρόπο καταπολέμησης ιομορφικού λογισμικού αποτελεί η επέκταση της δικαιοδοσίας των ιδιωτών σε θέματα κυβερνοεπιθέσεων. Πιο συγκεκριμένα, κάθε ιδιόκτητης συστήματος, ενεργώντας νόμιμα, δύναται να αστυνομεύει κατά ατόμων που θεωρεί εισβολείς στα συστήματα του (USAPA §217). Επιπλέον, οι πάροχοι υπηρεσιών διαδικτύου (ISPs) αποκτούν την δικαιοδοσία να αποκαλύπτουν *εθελοντικά* πληροφορίες των συνδρομητών τους με σκοπό την βοήθεια σε ποινικές έρευνες (USAPA §210).

Η πράξη νομικού περιεχομένου, με δεδομένο το ιστορικό πλαίσιο κατά το οποίο θεσπίστηκε, εισήγαγε μερικές αλλαγές που φαίνονται αναγκαίες και λογικές. Ωστόσο, παρόλη την ελευθερία που προσφέρει στην δράση κατά των κυβερνοεπιθέσεων σε ιδιώτες, ανάλογα τις συνθήκες μπορεί να ερμηνευτεί με διαφορετικό τρόπο και να οδηγήσει στην παραβίαση της ιδιωτικότητας προσωπικών δεδομένων πολιτών των ΗΠΑ. Είναι γεγονός ότι ο USAPA συγγράφηκε «εξαιρετικά γρήγορα», καθώς μόνο πέντε εβδομάδες πέρασαν από την παρουσίαση της πρώτης «πρόχειρης» έκδοσης και της νομικής θέσπισής του. Η πράξη είχε και εξακολουθεί να έχει σημαντικό αντίκτυπο στην προστασία των δικαιωμάτων ιδιωτικότητας των πολιτών. Πολλοί οργανισμοί που ειδικεύονται στην προστασία των ανθρώπινων δικαιωμάτων προβληματίζονται με το γεγονός ότι ο USAPA καταπατεί «απρεπώς» τα δικαιώματα στην ιδιωτικότητα των πολιτών των ΗΠΑ. (Nockleby, 2002)

3.3 Χονγκ-Κονγκ

Πριν μελετήσουμε την τρέχουσα νομοθεσία, τις δυνατότητες και τους περιορισμούς που αφορούν την καταπολέμηση του ιομορφικού λογισμικού στο Χονγκ Κονγκ είναι απαραίτητο να ορίσουμε το πολιτικό και ιστορικό πλαίσιο.

3.3.1 Ιστορικό και Πολιτικό πλαίσιο

Ιστορικά το Χονγκ Κονγκ ήταν αρχικά υπό βρετανικό έλεγχο και διέθετε πολιτικό και κυβερνητικό σύστημα που ήταν πολύ διαφορετικό από αυτό της κινεζικής κυβέρνησης. Το φιλελεύθερο πολιτικό σύστημα του ΧΚ έχει αναδείξει την περιοχή ως ένα από τα πιο σημαντικά κέντρα επιχειρηματικότητας παγκοσμίως, όπου προκύπτουν και ανθίζουν πολύτιμες ευκαιρίες κάθε είδους συνεργασίας αρκεί η περιοχή να ευνοείται από αυτές (Sucitawathi & Dewi, 2020). Τα δεδομένα άλλαξαν όταν την 1^{η} Ιουλίου του 1997 το Ηνωμένο Βασίλειο παραχώρησε την περιοχή του ΧΚ στην Λαϊκή Δημοκρατία της Κίνας (ΛΔΚ) υπό την προϋπόθεση ότι το ΧΚ θα ακολουθούσε κάθε ρύθμιση, πολιτική και κανόνα της κυβέρνησης της ΛΔΚ όσον αφορά το οικονομικό, πολιτικό, κοινωνικό, πολιτιστικό και αμυντικό κομμάτι. Η διαφορά στα δυο πολιτικά συστήματα (ΛΔΚ και ΧΚ) έκτοτε επιφέρει σύγκρουση συμφερόντων που εκτονώνεται με τη μορφή πολιτικής και κοινωνικής αναταραχής.

3.3.2 Νομικό πλαίσιο

Κατά τον νομικό οίκο Allen & Overy το ΧΚ δεν διαθέτει ολοκληρωμένο νόμο που να αφορά περιστατικά κυβερνοεπιθέσεων. Ωστόσο, σχετικές διατάξεις εντοπίζονται σε διάφορα καταστατικά. Η πρώτη προσπάθεια κατοχύρωσης των δικαιωμάτων προσωπικών δεδομένων από οντότητες που τα διαχειρίζονται ήταν το “PDPO” (*Personal Data (Privacy) Ordinance*). Θεσπίστηκε το 1995, τέθηκε σε εφαρμογή το 1996 και όρισε έξι αρχές (*DPP – Data Protection Principle*) που πρέπει να ακολουθεί κάθε διαχειριστής προσωπικών δεδομένων. Από τις σημαντικότερες για κάθε οργανισμό αποτελεί η τέταρτη (DPP 4), που υπαγορεύει ότι κάθε διαχειριστής προσωπικών δεδομένων πρέπει να ακολουθεί όλα τα απαραίτητα βήματα για να εξασφαλίσει την προστασία των προσωπικών δεδομένων έναντι μη εξουσιοδοτημένης ή τυχαίας επεξεργασίας, διαγραφής, απώλειας ή χρήσης τους.

Είναι γεγονός ότι το ΧΚ δεν διαθέτει συγκεκριμένη αρχή που να εφαρμόζει νόμους περί κυβερνοασφάλειας. Η αρχή PCPD (*Privacy Commissioner for Personal Data*) ιδρύθηκε με σκοπό την επιτήρηση και εφαρμογή του PDPO και έχει το δικαίωμα να ερευνήσει περιστατικά στα οποία αναφέρεται παραβίαση κάποιας παραγράφου του PDPO. Επιπλέον, παρακλάδι της Αστυνομίας του ΧΚ (HKPF – Hong Kong Police Force) το οποίο ειδικεύεται στην καταπολέμηση του ηλεκτρονικού εγκλήματος είναι το CSTCB (*Cyber Security and Technology Crime Bureau*). Είναι υπεύθυνο για τη διαχείριση περιστατικών κυβερνοασφάλειας, την διεξαγωγή ποινικών ερευνών και διατηρεί στενές σχέσεις με διεθνείς οργανισμούς καταπολέμησης εγκλήματος όπως η INTERPOL. Ωστόσο, έκπληξη προκαλεί ότι το CSTCB ιδρύθηκε μόλις το 2015, όταν ήδη από το 2011 οι αναφορές κυβερνοεπιθέσεων ολοένα και πλήθαιναν (Bower, et al., 2021).

Είναι σημαντικό να ειπωθεί ότι αρκετές φορές το PDPO παρερμηνεύεται ως σύνολο νόμων κυβερνοασφάλειας του Χονγκ Κονγκ. Όμως στην πραγματικότητα, το PDPO είναι ανεξάρτητο από την τεχνολογία που χρησιμοποιείται και καλύπτει προσωπικά δεδομένα που παρουσιάζονται σε κάθε είδος και μορφή, όχι μόνο ψηφιακή. Μείζονος σημασίας αποτελεί το γεγονός ότι το PDPO συγκεκριμένα δεν στοχεύει σε κυβερνοεγκλήματα που έχουν να κάνουν με άλλου είδους δεδομένα, όπως κλοπή εμπιστευτικών δεδομένων ή εμπορικά μυστικά ενός οργανισμού. Μέχρι στιγμής οι έννοιες «κυβερνοασφάλεια» και «κυβερνοέγκλημα» δεν έχουν οριστεί ρητώς σε καταστατικά και ερμηνεύονται ανάλογα το περιστατικό από τα δικαστήρια του ΧΚ (Chiu, 2020).

4. Συμπεράσματα

Έχοντας μελετήσει το ιομορφικό λογισμικό διαπιστώνει κανείς ότι δύναται να αποτελέσει σημαντικός κατασταλτικός παράγοντας των δραστηριοτήτων ενός οργανισμού στην κοινωνία της πληροφορίας του σήμερα. Η ραγδαία εξάπλωση των τεχνολογιών πληροφορικής και επικοινωνιών ώθησε όλες σχεδόν τις χώρες παγκοσμίως να θεσπίσουν σχετική νομοθεσία η οποία διαφέρει ως προς τον στόχο ανάλογα το κοινωνικό και πολιτικό περιβάλλον που επικρατεί στην κάθε περιοχή. Πρώτες οι ΗΠΑ δοκίμασαν να θέσουν νομικά υπό έλεγχο το ηλεκτρονικό έγκλημα με τη προσπάθεια να κορυφώνεται έπειτα από τις εξελίξεις της 11ης Σεπτεμβρίου. Όντας ένας από τους «γίγαντες» στον τομέα της Κυβερνοασφάλειας διεθνώς, οι ΗΠΑ προσφέρουν την δυνατότητα της αυτοπροστασίας και ιδιωτικής έρευνας έναντι κυβερνοεπιθέσεων, ενώ οι αρμόδιοι φορείς είναι παραπάνω από πρόθυμοι να ασχοληθούν σε βάθος εφ'όσον η υπόθεση αποδίδει καρπούς «ομοσπονδιακού ενδιαφέροντος». Από την άλλη πλευρά, το Χονγκ Κονγκ, υπό την σκιά μιας ερχόμενης περιόδου πολιτικής αστάθειας, επιχείρησε να θεσπίσει σε πρώτο στάδιο νομοθεσία με στόχο την προστασία προσωπικών δεδομένων. Ωστόσο, η έλλειψη απαραίτητων νόμων και ορισμών που αφορούν την κυβερνοασφάλεια από την πολιτεία είναι γεγονός. Επιπλέον, η ανάμειξη της Λαϊκής Δημοκρατίας της Κίνας στο εσωτερικό του Χονγκ Κονγκ με στόχο την πολιτική και οικονομική κυριαρχία έχει οδηγήσει σε ένα διττό πολιτικό σύστημα με απρόβλεπτες μελλοντικές εξελίξεις σε όλους τους ενδιαφερόμενους τομείς.

Πέρα από κάθε κοινωνικό, πολιτικό και νομικό πλαίσιο, οι μελέτες των ειδικών δείχνουν ότι η αντιμετώπιση των ζητημάτων ασφαλείας στις τεχνολογίες πληροφορικής και επικοινωνιών καθίσταται ολοένα και λιγότερο ορθολογική όταν ένας οργανισμός αυξάνει σε μέγεθος ή σε πολυπλοκότητα της πληροφοριακής του υποδομής ή όταν η επικινδυνότητα αυξάνεται. Γνωρίζοντας σε ένα πληροφοριακό σύστημα ότι η πιο αδύναμη συνιστώσα είναι ο ανθρώπινος παράγοντας, ο πιο διαχρονικός αμυντικός μηχανισμός αποτελεί «η προώθηση της κατάρτισης και ενημέρωσης των χρηστών σε θέματα ασφαλείας» (Γκρίτζαλης, 2019).

Βιβλιογραφία

Berr, J., 2017. *"WannaCry" ransomware attack losses could reach $4 billion,* s.l.: CBS Interactive Inc.

Bower, M., Cheung, F. H., Chan, K. & Huang, J., 2021. *A guide to Hong Kong's cyber security laws and practices.* s.l.:ALLEN & OVERY.

Brabant, M., 2006. *BBC News.* [Ηλεκτρονικό]
Available at: http://news.bbc.co.uk/2/hi/business/6182647.stm

Chiu, A., 2020. *Hong Kong: Cybersecurity Comparative Guide.* [Ηλεκτρονικό]
Available at: https://www.mondaq.com/hongkong/technology/963024/cybersecurity-comparative-guide

Cohen, F., 1987. Computer Viruses: Theory and Experiments. *Computers & Security,* 6(1), pp. 22-35.

Ghosh, A. K., 2001. *E-Commerce Security and Privacy.* s.l.:Kluwer Academic Publishers.

Jaikaran, C., 2021. *Cybersecurity: Selected Cyberattacks, 2012-2021,* s.l.: Congressional Research Service .

Malwarebytes, χ.χ. *WannaCry.* [Ηλεκτρονικό]
Available at: https://www.malwarebytes.com/wannacry

National Association Of Criminal Defense Lawyers, 2020. s.l.: s.n.

National Association Of Criminal Defense Lawyers, 2020. [Ηλεκτρονικό]
Available at: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

Nockleby, J., 2002. NTRODUCTION TO MODULE V: THE USA PATRIOT ACT, FOREIGN INTELLIGENCE SURVEILLANCE and CYBERSPACE PRIVACY. Στο: *Privacy in Cyberspace: 2002.* s.l.:Berkman Klein Center for Internet & Society at Harvard University.

Simon Kramer, J. C. B., 2010. A general definition of malware. *Journal in Computer Virology 6,* pp. 105-114.

Stafford, T. F. & Urbaczewski, A., 2004. Spyware: The Ghost in the Machine. *The Communications of the Assosiaction for Information Systems,* Τόμος 14.

Sucitawathi, P. & Dewi, I., 2020. The Hong Kong-China Government's Democratic Instability in terms of the Political Realism Perspective. *Journal of Etika Demokrasi,* Τόμος 5.

Γκρίτζαλης, Δ., 2019. *Αυτονομία και Ανυπακοή στον Κυβερνοχώρο.* 2η έκδοση επιμ. Αθήνα: NewTech Pub.

Σπινέλλης, Δ., Κοκολάκης, Σ. & Γκρίτζαλης, Σ., 1999. Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security,* Τόμος 7, pp. 121-128.