ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ασφάλεια Πληροφοριακών Συστημάτων

Εαρινό Εξάμηνο 2021-22

«Τοπικότητα των Κυβερνοαπειλών: Ιομορφικό Λογισμικό»

ΑΜΓΚΑΡ ΒΙΚΤΩΡ 3180007

ΚΟΝΤΟΔΗΜΑΣ ΧΡΗΣΤΟΣ-ΔΗΜΗΤΡΙΟΣ 3180083

Περιεχόμενα

Εισαγωγή

Ο Μη Κερδοσκοπικός Οργανισμός (ΜΚΟ) DigTech εδρεύει σε χώρα της Ευρωπαϊκής Ένωσης και αποτελεί έναν από τους πιο σημαντικούς φορείς στον χώρο της Κυβερνοασφάλειας. Ο DigTech είναι πιστοποιημένος κατά *ISO 9001:2008* και *ISO 27001:2013*, προσφέροντας εξατομικευμένες λύσεις για την ποιότητα και την ασφάλεια των παρεχόμενων υπηρεσιών.

Όντας εγκεκριμένοι Σύμβουλοι Ασφάλειας στον κυβερνοχώρο, ο DigTech καλείται να εξετάσει και να αξιολογήσει το βέλτιστο σενάριο με σκοπό να επιτευχθεί ομαλή επέκταση δραστηριοτήτων μεταξύ των Η.Π.Α. και του Χόνγκ-Κόνγκ. Έμφαση θα δοθεί στην οπτική, στις ανοχές και την διαχείριση τυχόν δράσεων στον Κυβερνοχώρο. Σημαντικό κριτήριο, θα αποτελέσει ένα πλέον μείζον ζήτημα της κυβερνοασφάλειας, το Ιομορφικό Λογισμικό. Θα αναλυθεί το εύρος μιας τέτοιας απειλής καθώς και οι εκάστοτε δυνατότητες και περιορισμοί για την αντιμετώπιση του Ιομορφικού Λογισμικού.

Ιομορφικό Λογισμικό

Το **Ιομορφικό Λογισμικό**, αποτελεί ένα σύγχρονο πρόβλημα της κοινωνίας και συγκεκριμένα των επιχειρήσεων ή των μη κερδοσκοπικών οργανισμών όπως της DigTech διότι είναι το μέσο που χρησιμοποιούν συνήθως οι hackers ώστε να υποκλέψουν δεδομένα ή να μειώσουν την απόδοση των συστημάτων που διαθέτουν οι οργανισμοί με στόχο να επωφεληθούν από αυτό. Το κακόβουλο αυτό λογισμικό όταν εκτελείται προκαλεί άμεσα ή έμμεσα ενέργειες οι οποίες δεν είναι γνωστές για το άτομο που διαθέτει το σύστημα. Αυτό συνηθώς ενεργοποιείται, όταν άθελα από τον χρήστη του ηλεκτρονικού υπολογιστή, εκτελεί το πρόγραμμα που το διαθέτει.

Εικόνα 1: Ιομορφικό Λογισμικό

Οι κύριοι τύποι του Ιομορφικού Λογισμικού, που επηρεάζουν τα περισσότερα συστήματα του πλανήτη και πρέπει οι χώρες να δώσουν ιδιαίτερη προσοχή, είναι τρεις και είναι οι εξής παρακάτω:

1. Ο **Δούρειος Ίππος (Trojan)** έχει την δυνατότητα να παραπλανήσει το χρήστη και να τον πείσει να εκτελέσει το αρχείο που έχει κατεβασμένο στον υπολογιστή του. Χρησιμοποιείται κυρίως όταν ο επιτήδειος θέλει να υποκλέψει δεδομένα που θεωρεί ο ίδιος σημαντικά ή να αποκτήσει τον έλεγχο του συστήματος.

2. Το **Σκουλήκι (Worm)** έχει την ικανότητα να πολλαπλασιαστεί σ' ένα σύστημα αυτόματα και με αυτόν τον τρόπο στοχεύει στην απόκτηση στοιχείων όπως κωδικοί πρόσβασης οι οποίοι αποστέλλονται σε αυτόν που κάνει την επίθεση και έτσι να έχει πρόσβαση στο δίκτυο. Συνήθως, για να εγκατασταθεί στον υπολογιστή του θύματος, ο θύτης στέλνει μήνυμα μέσω email ώστε ο παραλήπτης να πέσει στην παγίδα του.

3. Το **Πρόγραμμα Ιός (Virus)** έχει την δυνατότητα να συνυπάρχει με άλλο εκτελέσιμο πρόγραμμα ώστε να πραγματοποιεί ενέργειες μόνο όταν ο χρήστης το εκτελεί. Μπορεί να προκαλέσει διάφορες συνέπειες όπως καταστροφή προγραμμάτων, διαγραφή αρχείων, μορφοποίηση (format) του αποθηκευτικού χώρου, αδυναμία εκκίνησης του ηλεκτρονικού υπολογιστή, ελάττωση της ανταπόκρισης του συστήματος, προβλήματα στη λειτουργία των εγκατεστημένων εφαρμογών και εμφάνιση ενοχλητικών μηνυμάτων στην επιφάνεια εργασίας του χρήστη.

Στο παρακάτω πίνακα παρουσιάζονται συνοπτικά κάποιοι από τους υπόλοιπους τύπους Ιομορφών οι οποίοι είναι εξίσου επικίνδυνοι με τους άλλους και μπορούν να προκαλέσουν μεγάλη ζημιά στις εταιρείες:

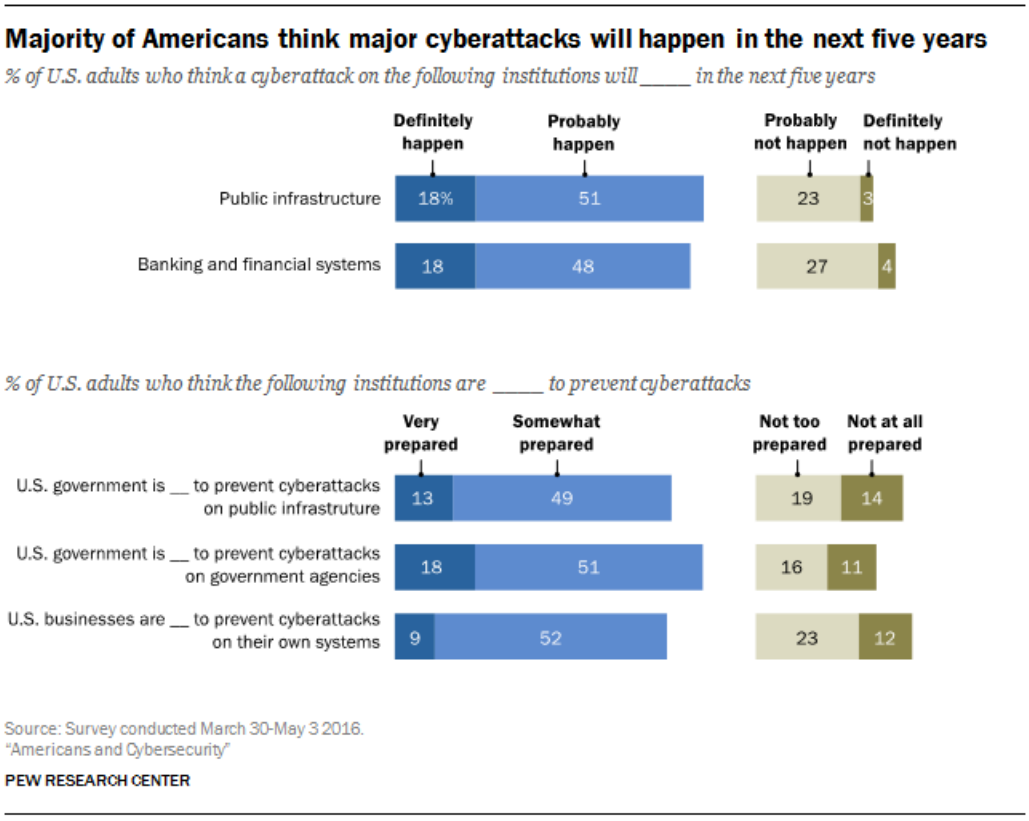
ΤΥΠΟΣ	**ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ**
Κρυπτογραφημένος Ιός	Περιέχει κρυπτογραφημένο κώδικα
Πολυμορφικός Ιός	Αλλάζει μορφή
Πολυμερής Ιός	Μολύνει εφαρμογές

Πίνακας 1: Τύποι Ιομορφών

Οπτική σε Ζητήματα Κυβερνοασφάλειας

Αρκετοί είναι οι πολίτες της Αμερικής οι οποίοι έχουν συνδέσει την έννοια του «χάκερ» με την εικόνα ενός κακόβουλου εγκληματία. Στην πραγματικότητα, ένας χάκερ μπορεί να προσδιορισθεί μόνο από τις προθέσεις του. Από την μεριά των επιχειρήσεων, αυτό φαίνεται να έχει γίνει περισσότερο αντιληπτό, καθώς πλέον κάθε οργανισμός φαίνεται να απορρίπτει την προηγούμενη εικόνα του χάκερ και να τον προσεγγίζει ως σύμβουλο ασφάλειας με την έννοια του Penetration Tester.

Στις Η.Π.Α. τα συχνά περιστατικά κυβερνοεπιθέσεων έχουν προκαλέσει ιδιαίτερη ανησυχία στην κοινωνία. Σύμφωνα με πρόσφατες έρευνες, οι Αμερικάνοι πολίτες φαίνεται πως περιμένουν αύξηση των κυβερνοεπιθέσεων μέσα στα επόμενα χρόνια. Η οπτική τους για την διαχείριση τέτοιων κρίσεων ποικίλει με βάση την ηλικία, καθώς οι νέοι είναι περισσότερο αισιόδοξοι ως προς τον βαθμό αντιμετώπισης και την ορθή διαχείριση της κατάστασης που μπορεί να επιτευχθεί από την μεριά της Πολιτείας.



Εικόνα 2: Οπτική Η.Π.Α. απέναντι σε κυβερνοεπιθέσεις

Η κοινωνία των Η.Π.Α., φαίνεται να θεωρεί τις κυβερνήσεις της Κίνας και της Ρωσίας μεγαλύτερη απειλή για την κυβερνοασφάλεια της χώρας της σε σχέση με άλλες ξένες κυβερνήσεις ή μη κυβερνητικές ομάδες και άτομα. Όσον αφορά τις πιθανές πηγές επιθέσεων, φαίνεται να υπάρχει διάκριση ανάμεσα στην πολιτική τους ταυτότητα. Οι Δημοκρατικοί, είναι περισσότερο πιθανό από τους Ρεπουμπλικάνους να θεωρήσουν τη ρωσική κυβέρνηση ως μεγαλύτερη απειλή (79% έναντι 70%).

Στην κοινωνία του Χόνγκ-Κόνγκ, τα περιστατικά κυβερνοεπιθέσεων έχουν σημειώσει ιδιαίτερη αύξηση από το ξέσπασμα του Covid-19. Συγκεκριμένα, σύμφωνα με στατιστικά δεδομένα φαίνεται να έχει υπάρξει σημαντική αύξηση του κυβερνοεγκλήματος κατά 55% από το 2019. Οι επιχειρήσεις φαίνονται να βρίσκονται σε επαγρύπνηση, καθώς λαμβάνουν συνεχώς όλο και περισσότερα μέτρα με σκοπό να προστατευθούν σε μια επικείμενη απειλή.

Η ραγδαία αύξηση του Ιομορφικού Λογισμικού, έχει ωθήσει αρκετούς τομείς του Χόνγκ-Κόνγκ στην λήψη απαραίτητων μέτρων προστασίας και ανάκαμψης. Μερικοί από αυτούς είναι ο Χρηματοοικονομικός, ο Τραπεζικός, ο Ασφαλιστικός καθώς και γενικότερα οι επιχειρήσεις ανεξαρτήτου οικονομικού μεγέθους και χαρακτήρα. Η στάση τους απέναντι στην καταπολέμηση των Ιομορφών, έχει οδηγήσει επιτυχώς σε μια προσπάθεια αφύπνισης κατά των κυβερνοεγκλημάτων. Χαρακτηριστικό παράδειγμα αποτελεί ο Τραπεζικός τομέας του Χόνγκ-Κόνγκ, καθώς μέσω της θέσπισης του Cybersecurity Fortification Initiative (CFI) το 2016 και της επιτυχούς αναβάθμισής του στο CFI 2.0 το 2021, στοχεύει στο να αυξήσει την ανθεκτικότητα του Τραπεζικού τομέα στον κυβερνοχώρο σε υψηλότερα επίπεδα.

Ανοχές σε Ζητήματα Κυβερνοασφάλειας

Οι περισσότερες ασιατικές χώρες έχουν δημιουργήσει νομοθεσία ειδικά για το έγκλημα στην κυβερνοασφάλεια. Ωστόσο, το **Χονγκ-Κονγκ** σ' αυτό το τομέα έχει μείνει πίσω με αποτέλεσμα να μην διαθέτει επίσημα αυτόνομη νομοθεσία για την ασφάλεια στον κυβερνοχώρο και δυστυχώς δεν προβλέπεται από τους κυβερνόντες να τη θεσπίσουν στο κοντινό μέλλον. Ωστόσο, το αστυνομικό τμήμα του Χονγκ-Κονγκ έχει αναλάβει να δημιουργήσει νόμους για την αποτροπή υποκλοπής ή διαγραφής δεδομένων και καταστροφής περιουσίας από ένα άτομο σε ένα τρίτο.

Πιο αναλυτικά, με το **άρθρο 161** του διατάγματος, είναι αδίκημα ένα άτομο να έχει πρόσβαση σε υπολογιστή με πρόθεση **α)** να αποκομίσει ανέντιμα κέρδος, **β)** να υποκλέψει αρχεία**, γ)** ή και να προκαλέσει απώλεια δεδομένων σε κάποιον τρίτο. Επίσης, σύμφωνα με τα **άρθρα 7, 11(3A)** και **16A**, όποιο πρόσωπο βρεθεί με αρχεία στον υπολογιστή του, στα οποία δεν έχει άδεια πρόσβασης, μπορεί να θεωρηθεί ένοχος για κλοπή ή για απάτη. Επιπλέον, σύμφωνα με τα **άρθρα 59** και **60** του διατάγματος, τα οποία αναφέρονται στην καταστροφή περιουσίας ενός προσώπου από τρίτο, αν προκληθεί βλάβη στον ηλεκτρονικό υπολογιστή του, η οποία δεν οφείλεται από την κακή χρήση που του κάνει αλλά από άλλους εξωγενείς παράγοντες όπως, παραδείγματος χάριν η εγκατάσταση ενός προγράμματος που περιέχει Ιομορφικό Λογισμικό, τότε θεωρείται αδίκημα και κατατάσσεται στη κατηγορία του εμπρησμού. Τέλος, το Χονγκ Κονγκ δεν διαθέτει νόμο ο οποίος να απαγορεύει την αποθήκευση παράνομου υλικού από τον επιτιθέμενο σ' ένα σύστημα που δεν έχει εξουσιοδότηση για πρόσβαση. Ωστόσο, σύμφωνα με το **άρθρο 159A,** αν ο διαχειριστής του συστήματος γνωρίζει ότι διαθέτει τέτοια παράνομα αρχεία στον υπολογιστή του, θεωρείται ότι είναι ένοχος συνωμοσίας για την διάπραξη τέτοιων αδικημάτων.

Ο παρακάτω πίνακας δείχνει τις ποινές που έχει το πρόσωπο που καταπατά τους νόμους που αναφέρθηκαν παραπάνω του Χονγκ-Κονγκ για τον περιορισμό της επίθεσης συστημάτων με Ιομορφικό Λογισμικό.

ΝΟΜΟΣ	**ΠΟΙΝΗ**
ΑΡΘΡΟ 161 ΤΟΥ ΔΙΑΤΑΓΜΑΤΟΣ	ΦΥΛΑΚΙΣΗ ΠΕΝΤΕ ΧΡΟΝΙΑ
ΑΡΘΡΟ 7, 11(3A) & 16A ΤΟΥ ΔΙΑΤΑΓΜΑΤΟΣ	ΦΥΛΑΚΙΣΗ ΕΦΤΑ ΧΡΟΝΙΑ
ΑΡΘΡΟ 59 & 60 ΤΟΥ ΔΙΑΤΑΓΜΑΤΟΣ	ΦΥΛΑΚΙΣΗ ΔΕΚΑ ΧΡΟΝΙΑ Ή ΙΣΟΒΙΑ
ΑΡΘΡΟ 159A ΤΟΥ ΔΙΑΤΑΓΜΑΤΟΣ	ΦΥΛΑΚΙΣΗ ΠΕΝΤΕ ΧΡΟΝΙΑ

Πίνακας 2: Ποινές στο Χόνγκ-Κόνγκ

Στις **Ηνωμένες Πολιτείες Αμερικής**, δεν έχουν μια αυτόνομη νομοθεσία που να ρυθμίζει και να καλύπτει την ασφάλεια όλης της χώρας στον κυβερνοχώρο. Κάθε πολιτεία της Αμερικής έχει τους δικούς της νόμους στο τομέα αυτό και έχει ως συνέπεια κάθε επιχείρηση ή οργανισμός που θέλει να επεκτείνει τις δραστηριότητές της στη χώρα αυτή, όπως η ΜΚΟ DigTech, να είναι πολύ προσεκτική και να συμμορφώνεται με τις αλλαγές του νόμου ώστε να μην βρεθεί αντιμέτωπη με κυρώσεις. Ωστόσο, υπάρχουν νομοσχέδια τα οποία καλύπτουν τα πιο βασικά εγκλήματα στο κυβερνοχώρο και θα αναφερθούν κάποια από αυτά παρακάτω.

Ο **ομοσπονδιακός νόμος 18 USC § 1030** περί απάτης και κατάχρησης υπολογιστών (CFAA), ο οποίος θεσπίστηκε το 1984 και άλλαξε το 1986, περιλαμβάνει αρκετούς κανόνες όπου περιορίζουν κατά μεγάλο ποσοστό το Κυβερνοέγκλημα. Παρακάτω, θα επισημάνουμε κάποιους από αυτούς που έχουν να κάνουν σχέση με την απειλή του Ιομορφικού Λογισμικού.

Αναλυτικότερα, απαγορεύει στο άτομο να έχει πρόσβαση σε υπολογιστή που δεν έχει εξουσιοδότηση και να αποκτήσει πληροφορίες εθνικής ασφάλειας. Επίσης, το πρόσωπο που προκαλεί βλάβη σε υπολογιστή με τρόπο όπως, τη δημιουργία μολυσμένου προγράμματος και εγκατάσταση του στον ανυποψίαστο χρήστη ο οποίος είναι κάτοχος της ηλεκτρονικής συσκευής, διαπράττει έγκλημα και διώκεται ποινικά. Επιπλέον, δεν επιτρέπεται ο εκβιασμός για πρόκληση ζημιάς στον υπολογιστή του ατόμου και την υποκλοπή ή καταστροφή δεδομένων. Τέλος, απαγορεύεται η απόκτηση και η διακίνηση δεδομένων από υπολογιστή τρίτου.

Ο **ομοσπονδιακός νόμος 18 USC § 2702** για την προστασία των ηλεκτρονικών επικοινωνιών (ECPA), ο οποίος αρχικά θεσπίστηκε το 1968 και άλλαξε το 1986 λόγω της εξέλιξης της τεχνολογίας, προστατεύει το απόρρητο του περιεχομένου των αρχείων που αποστέλλονται μέσω των υπηρεσιών emails.

Οι ποινές, όταν παραβιάζονται οι παραπάνω κανόνες των ομοσπονδιακών νόμων, βρίσκονται στο παρακάτω πίνακα:

ΟΜΟΣΠΟΝΔΙΑΚΟΣ ΝΟΜΟΣ	**ΚΑΝΟΝΕΣ**	**ΠΟΙΝΗ**
ΝΟΜΟΣ 18 USC § 1030	1) ΠΡΟΣΒΑΣΗ ΣΕ ΥΠΟΛΟΓΙΣΤΗ ΧΩΡΙΣ ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΙ ΚΛΟΠΗ ΔΕΔΟΜΕΝΩΝ ΕΘΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ 2) ΒΛΑΒΗ ΣΕ ΥΠΟΛΟΓΙΣΤΗ	1) ΦΥΛΑΚΙΣΗ 10 ΕΤΗ 2) ΦΥΛΑΚΙΣΗ ΕΩΣ 5 ΕΤΗ

	3) ΕΚΒΙΑΣΜΟΣ ΓΙΑ ΒΛΑΒΗ ΥΠΟΛΟΓΙΣΤΗ Ή ΥΠΟΚΛΟΠΗ ΔΕΔΟΜΕΝΩΝ 4) ΔΙΑΚΙΝΗΣΗ ΔΕΔΟΜΕΝΩΝ	3) ΦΥΛΑΚΙΣΗ ΕΩΣ 5 ΕΤΗ 4) ΦΥΛΑΚΙΣΗ ΕΝΟΣ ΕΤΟΥΣ
ΝΟΜΟΣ 18 USC § 2702	-	ΦΥΛΑΚΙΣΗ ΕΩΣ 10 ΕΤΗ

Διαχείριση Δράσεων Κυβερνοασφάλειας:

Στην περίπτωση των ΗΠΑ, κατά τη διάρκεια επιθέσεων στον κυβερνοχώρο, το Υπουργείο Εσωτερικής Ασφάλειας (DHS) παρέχει βοήθεια, ερευνά τους υπεύθυνους και συντονίζει την εθνική απόκριση.

Στις 26 Ιουλίου 2016, ο Πρόεδρος Ομπάμα υπέγραψε την Οδηγία Προεδρικής Πολιτικής (PPD) 41, η οποία ορίζει αρχές για την απάντηση σε οποιοδήποτε περιστατικό στον κυβερνοχώρο καθώς και για σημαντικές υποθέσεις.

Οι ΗΠΑ ορίζουν τρεις γραμμές σε περίπτωση κυβερνοεπίθεσης, οι οποίες δεν διαχειρίζονται αποκλειστικά από κανέναν οργανισμό:

1. Απόκριση Αγαθών, παροχή τεχνικών πόρων για ανάκαμψη από συμβάν μέσω του National Cybersecurity and Communication Integration Center (NCCIC).
2. Απόκριση Απειλών, έρευνα συμβάντος από Department of Justice (DOJ), FBI και National Cyber Investigative Joint Task Force (NCIJTF)
3. Πληροφοριακή Υποστήριξη, ευαισθητοποίηση γύρω από περιστατικά κυβερνοεπίθεσης μέσω των Office of the Director of National Intelligence (OPNI) και Cyber Threat Intelligence Integration Center (CTIIC)

Στην περίπτωση του Χόνγκ Κόνγκ, ομοίως δεν υπάρχει κάποιος αποκλειστικός φορέας για τη διαχείριση κυβερνοεπιθέσεων καθώς απαιτείται μια συλλογική δράση.

Η Αστυνομία του Χόνγκ Κόνγκ (HKPF), αποτελεί τον κύριο φορέα σε οποιοδήποτε θέμα σχετίζεται με ηλεκτρονικά εγκλήματα. Είναι υπεύθυνη για την επιβολή των κυρώσεων, για την διεξαγωγή έρευνας του συμβάντος, η οποία περιλαμβάνει αναζήτηση και κατάσχεση στοιχείων εντός δημοσίου και ιδιωτικού χώρου καθώς και σύλληψη πιθανών ύποπτων.

Η αστυνομία του Χόνγκ Κόνγκ μπορεί να χρειαστεί την βοήθεια της INTERPOL για την αντιμετώπιση κυβερνοεπιθέσεων με δράστες εκτός των συνόρων της χώρας.

Το Cyber Security and Technology Crime Bureau (CSTB), είναι επίσης υπεύθυνο για την διαχείριση κυβερνοεπιθέσεων καθώς και την αποτροπή αλλά και έρευνα τέτοιων συμβάντων.

Δυνατότητες Αντιμετώπισης Ιομορφικού Λογισμικού

Οι **Ηνωμένες Πολιτείες Αμερικής** ξοδεύουν κάθε χρόνο πολλά εκατομμύρια για την ασφάλεια στον κυβερνοχώρο ώστε να καταπολεμήσει τις απειλές που έχουν καθημερινά από τους hackers. Με αυτό το χρηματικό ποσό που παρέχει σ' αυτό το τομέα, έχει ως αποτέλεσμα, η χώρα να διαθέτει πολλά συστήματα και ομάδες ατόμων που βοηθάνε στην ανίχνευση εισβολής και στην καταπολέμησή της.

Πιο αναλυτικά, η ομάδα ετοιμότητας έκτακτης ανάγκης υπολογιστών (US – CERT) προσφέρει υποστήριξη ώστε η χώρα να αμύνεται σε επιθέσεις στον κυβερνοχώρο δηλαδή παρατηρεί κινήσεις στα δίκτυα και εντοπίζει μη φυσιολογικές δραστηριότητες. Η ομάδα Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) παρέχει βοήθεια σε ιδιοκτήτες επιχειρήσεων και αποκρίνεται σε απειλές στον κυβερνοχώρο. Το Υπουργείο Εσωτερικής Ασφάλειας (DHS) διαθέτει το σύστημα EINSTEIN που αρχικά προστάτευε μόνο τα στρατιωτικά δίκτυα και διευκόλυνε την κυβέρνηση των ΗΠΑ να έχει σε πραγματικό χρόνο προειδοποίηση για εισβολή στο δίκτυο και έτσι να μπορεί να σταματήσει την κακόβουλη δραστηριότητά της. Το 2008 όμως, το αναβάθμισαν και το EINSTEIN 2, όπως αποκαλείται, εξυπηρετεί τους ομοσπονδιακούς οργανισμούς για να προστατεύσει τους υπολογιστές τους, τα δίκτυα και τα δεδομένα τους από τυχόν επιθέσεις. Αυτή την χρονική περίοδο αναπτύσσεται η τρίτη φάση του EINSTEIN όπου θα μπορεί να ανιχνεύει και να διακόπτει αυτόματα κακόβουλες δραστηριότητες πριν προκληθεί ζημιά σε συστήματα και δίκτυα εταιρειών. Τέλος, το Υπουργείο Εθνικής Ασφάλειας (DHS) μέσα στα χρόνια έχει προσλάβει περισσότερους από 230 επαγγελματίες που ασχολούνται για την ασφάλεια στον κυβερνοχώρο ώστε να έχει πιο αποτελεσματικότερη αντιμετώπιση σε απειλές όπως το Ιομορφικό Λογισμικό.

Το **Χονγκ-Κονγκ** σε σχέση με την Αμερική, δεν δαπανά το ίδιο χρηματικό ποσό για την κυβερνοασφάλεια. Ωστόσο, για να διαχειριστεί τις επιθέσεις στο κυβερνοχώρο, έχει δημιουργήσει ομάδες ανθρώπων οι οποίες υποστηρίζουν τους οργανισμούς για την προστασία των δεδομένων τους και ειδοποιούν ή αντιμετωπίζουν παράνομες ενέργειες που βλάπτουν την ασφάλεια της χώρας.

Πιο συγκεκριμένα, η OGCIO (Κυβερνητικό Γραφείο Αντιμετώπισης Περιστατικών και Ασφάλειας Πληροφοριών), η HKCERT (Κέντρο Συντονισμού της Ομάδας Αντιμετώπισης Έκτακτης Ανάγκης Υπολογιστών του Χονγκ Κονγκ) και πολλές άλλες, συνεργάζονται για να παρέχουν πληροφόρηση στους οργανισμούς σχετικά με τα μέτρα που πρέπει να πάρουν για να είναι ασφαλείς σε μια υποτιθέμενη κυβερνοεπίθεση. Αναλυτικότερα, η HCKERT διαθέτει 24ωρη τηλεφωνική γραμμή για να λαμβάνει αναφορές για συμβάντα ασφάλειας και παρέχει συμβουλές για το πως θα αντιμετωπίσουν αποτελεσματικότερα τις επιθέσεις και για το πως θα

κάνουν την ανάκτηση των δεδομένων τους που πιθανόν μπορεί να έχουν διαγραφεί λόγω της ύπαρξης κακόβουλου λογισμικού. Επίσης, διοργανώνει σεμινάρια για τις εταιρείες ώστε να τις ευαισθητοποιήσει και να τους μάθει πρακτικές για να αμύνονται από μία επίθεση. Τέλος, θα δούμε κάποιους κανόνες – συμβουλές που δίνουν ώστε να αποφύγουν τις αρνητικές συνέπειες του Ιομορφικού Λογισμικού και οι οποίοι είναι οι εξής: 1) οι μηχανές ανίχνευσης και επισκευής που διαθέτουν θα ενημερώνονται τακτικά και όποτε είναι απαραίτητο, 2) αρχεία που δεν είναι γνωστή η πηγή προέλευσής τους, θα απορρίπτονται ή θα ελέγχονται για την ύπαρξη κακόβουλου λογισμικού, 3) να υπάρχουν αντίγραφα ασφαλείας ώστε να μην χαθούν πληροφορίες του οργανισμού και 4) οι χρήστες – εργαζόμενοι απαγορεύεται να δημιουργούν, να διαδίδουν ή να εκτελούν εν γνώση τους Ιομορφικό Λογισμικό το οποίο μπορεί να βλάψει την εταιρεία του ή άλλους οργανισμούς.

Περιορισμοί Αντιμετώπισης Ιομορφικού Λογισμικού

Οι περιορισμοί στην αντιμετώπιση του Ιομορφικού Λογισμικού και στις δύο χώρες (καθώς και στις περισσότερες) φαίνονται να είναι κοινοί.

Η έλλειψη ενός αποκλειστικού φορέα, μπορεί να σταθεί εμπόδιο στην αντιμετώπιση μιας κυβερνοεπίθεσης, καθώς η επικοινωνία που απαιτείται για τον συγχρονισμό και την ομαλή διαχείριση μιας τέτοιας κρίσης, είναι ύψιστης σημασίας και ακεραιότητας.

Η ευαισθητοποίηση σε θέματα «καλής υγιεινής» κατά την προφύλαξη από κακόβουλο λογισμικό φαίνεται να είναι χαμηλότερη από τα επιθυμητά επίπεδα. Δυστυχώς, αρκετές είναι οι περιπτώσεις όπου η αφύπνιση έχει παρέλθει μετά από μια τέτοια επιβεβαιωμένη κρίση.

Παραδείγματος χάριν, αποτελούν οι πλέον διαδεδομένες επιθέσεις Ιομορφικού Λογισμικού “ransomware” οι οποίες πλήττουν και τις δύο χώρες. Η σημασία καθώς και το εύρος της απειλής μιας τέτοιας επίθεσης είναι ιδιαίτερα ανησυχητικό. Συγκεκριμένα, ένα παράδειγμα τέτοιο κακόβουλου λογισμικού αποτελεί αυτό του WannaCry.

Στην περίπτωση των ΗΠΑ, σπουδαίο παράδειγμα αποτελεί η υπόθεση των Colonial Pipeline. Συγκεκριμένα, ο περιορισμός της αντιμετώπισης βρισκόταν στο γεγονός ότι η εταιρεία δεν είχε εξασφαλίσει την δημιουργία τακτικών αρχειοθετήσεων (backup) των κρίσιμων υποδομών της.

Ομοίως, το Χόνγκ Κόνγκ φαίνεται να έχει υποφέρει στο παρελθόν από το ίδιο Ιομορφικό Λογισμικό. Δυστυχώς, στη συγκεκριμένη περίπτωση η μοναδική λύση του προβλήματος είναι η ορθή πρόληψη.

Επίλογος

Εν κατακλείδι, και οι δύο χώρες που αναλύσαμε παραπάνω έχουν τις δυνάμεις για να καταπολεμήσουν τις επιθέσεις στο κυβερνοχώρο από τους επιτήδειους hackers που θέλουν να υποκλέψουν δεδομένα χρήσιμα γι' αυτούς χρησιμοποιώντας Ιομορφικό Λογισμικό. Ωστόσο, η Αμερική έχει επενδύσει πολλά χρήματα πάνω σ' αυτό τομέα και είναι οργανωμένη και έμπειρη χρησιμοποιώντας κατάλληλες τεχνολογίες για να αποτρέψει τέτοιες επιθέσεις. Πιστεύουμε ότι ο Μη Κερδοσκοπικός Οργανισμός DigTech είναι προτιμότερο να επεκτείνει τις δραστηριότητές του στις Ηνωμένες Πολιτείες Αμερικής έχοντας υπόψιν του τους νόμους που αλλάζουν σε κάθε πολιτεία.

Πηγές

1. CISA Cyber Incident Response
2. A guide to Hong-Kong's Cyber Security Laws and Practices
3. DHS Role in Cyber Incident Response
4. Ransomware Attack | Hong Kong Police Force
5. Americans' views about cybersecurity policy | Pew Research Center
6. The Public Is Highly Concerned About Cyber Attacks on the United States
7. RSA-Survey-Report-FINAL.pdf | Kaspersky.com
8. Top Tips to Prevent and Handle Cyber Incidents in Hong-Kong
9. Privacy Civil Liberties
10. Computer Fraud and Abuse Act
11. Federal Cybersecurity and Privacy Laws
12. Cybersecurity Laws and Regulations
13. State Cybercrime Legislation in the United States of America
14. Cyber Security Around the World
15. Hong-Kong Crimes Ordinance
16. The Privacy Data Protection and Cybersecurity Law Review
17. Information Cyber Security
18. Preventing and Defending Against Cyber Attacks