Ασφάλεια Πληροφοριακών Συστημάτων

«Ιομορφικό Λογισμικό»

Μελάς Παναγιώτης 3190118

Φιλιππακόπουλος Αλέξης 3190212

Γεωργιάδης Ελευθέριος 3190031

Υπεύθυνος Καθηγητής : Γκρίτζαλης Δημήτρης

Γραπτή Εργασία Προόδου *Εαρινό Εξάμηνο 2021-22*

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1 ΠΡΟΛΟΓΟΣ

Η ραγδαία και συνεχιζόμενη ψηφιοποίηση όλων των πτυχών της σύγχρονης ζωής επηρεάζει άμεσα ολόκληρη την κοινωνικοπολιτική σύσταση και δομή . Με την αυξανόμενη χρήση του διαδικτύου και τον τεράστιο όγκο δεδομένων και πληροφορίας, οι κυβερνητικές βάσεις δεδομένων έχουν τοποθετηθεί ως κύριοι στόχοι για χάκερ και πράξεις κυβερνοπολέμου. Ενός κυβερνοπολέμου που αφορά τόσο τις διαμάχες και τα συμφέροντα εθνών-κρατών με στόχο την διείσδυση και την πρόκληση ζημίας ή διαταραχών στην πληροφορία άλλων εθνών, όσο και μη κρατικούς φορείς, όπως τρομοκρατικές ομάδες, εταιρείες, πολιτικές ή ιδεολογικές εξτρεμιστικές ομάδες, εγκληματικές οργανώσεις και χακτιβιστές.

Τι είναι το ιομορφικό λογισμικό;

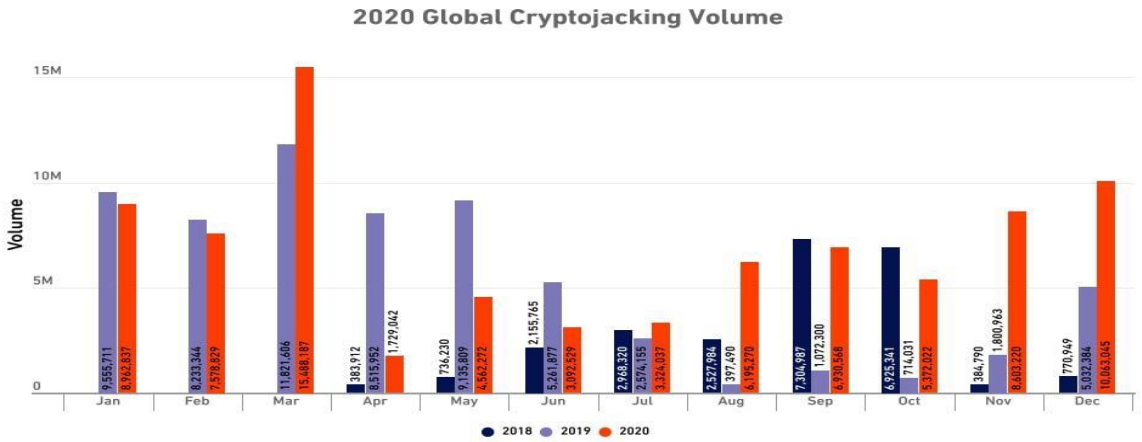
Το ιομορφικό λογισμικό, ή αλλιώς «κακόβουλο λογισμικό» (malware), αναφέρεται σε οποιοδήποτε παρεμβατικό λογισμικό που έχει αναπτυχθεί από εγκληματίες του κυβερνοχώρου (συχνά αποκαλούμενοι «χάκερ») για την κλοπή δεδομένων και την καταστροφή ή την καταστροφή υπολογιστών και συστημάτων υπολογιστών. Παραδείγματα κοινών κακόβουλων προγραμμάτων περιλαμβάνουν ιούς, ιούς τύπου worm, ιούς trojan, spyware, adware και ransomware. Οι πρόσφατες επιθέσεις κακόβουλου λογισμικού έχουν συγκεντρώσει δεδομένα σε μαζικές ποσότητες.

Συνήθεις τύποι ιομορφικού λογισμικού τα τελευταία χρόνια.

Virus/Ιός: Ένας ιός είναι ένας τύπος κακόβουλου λογισμικού που συνδέεται με ένα έγγραφο ή αρχείο που υποστηρίζει μακροεντολές για την εκτέλεση του κώδικά του και τη διάδοση από κεντρικό υπολογιστή σε κεντρικό υπολογιστή. Μόλις γίνει λήψη, ο ιός θα παραμείνει αδρανής μέχρι να ικανοποιηθεί κάποια προκαθορισμένη συνθήκη (πχ να ανοίξει το αρχείο ο χρήστης). Οι ιοί έχουν σχεδιαστεί για να διαταράσσουν την ικανότητα λειτουργίας ενός συστήματος. Ως αποτέλεσμα, οι ιοί μπορούν να προκαλέσουν σημαντικά λειτουργικά προβλήματα και απώλεια δεδομένων.

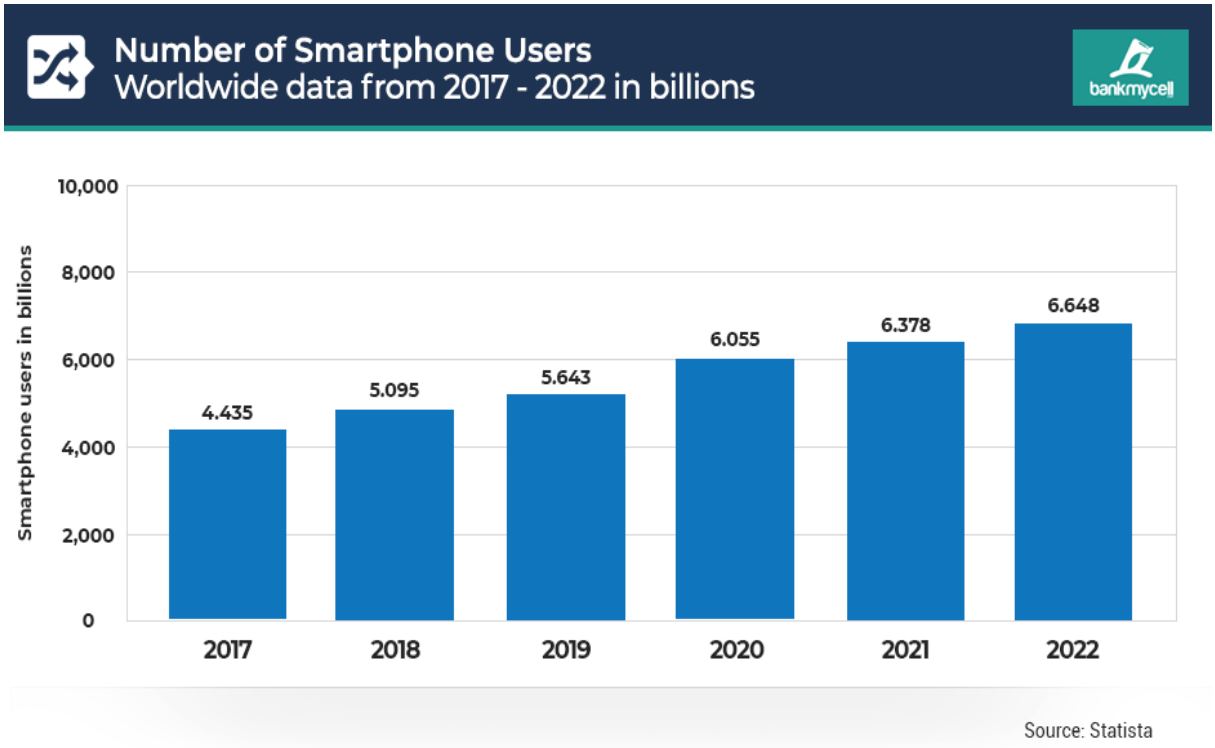
Cryptomining malware/λογισμικό εξόρυξης κρυπτονομισμάτων:

Το λογισμικό εξόρυξης κρυπτονομισμάτων έχει σχεδιαστεί για να εκμεταλλεύεται το γεγονός ότι ορισμένα κρυπτονομίσματα πληρώνουν τους εξορύκτες για την επίλυση υπολογιστικών γρίφων Proof of Work. Το cryptomining malware χρησιμοποιεί τους πόρους CPU/GPU του μολυσμένου υπολογιστή για να λύσει αυτά τα προβλήματα, κερδίζοντας χρήματα για τον χειριστή κακόβουλου λογισμικού. Σε όλο τον κόσμο, το κακόβουλο λογισμικό κρυπτογράφησης αντιπροσωπεύει το 22% των επιθέσεων κακόβουλου λογισμικού με το XMRig ως την πιο κοινή παραλλαγή.

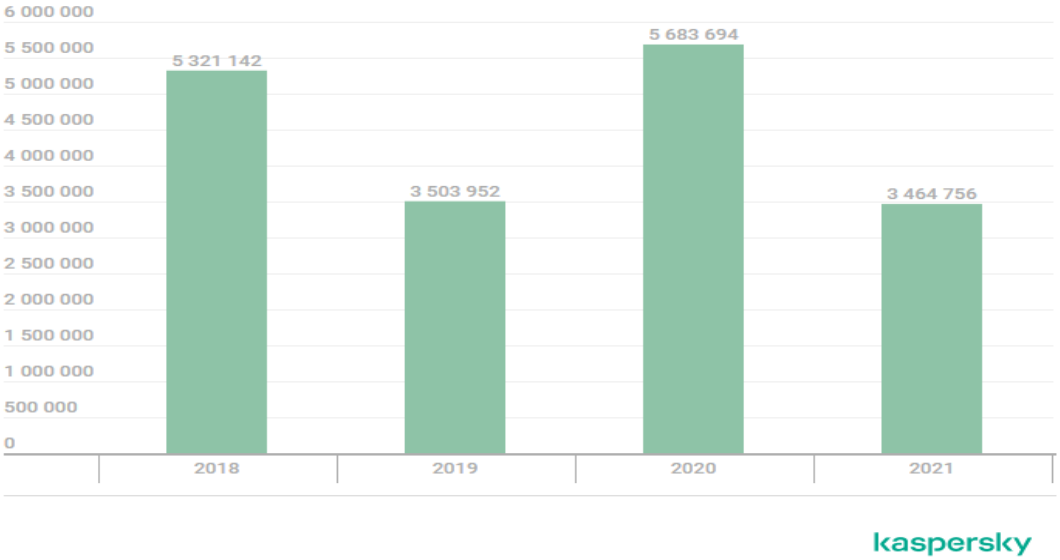


Mobile malware: Το Android είναι το πιο δημοφιλές λειτουργικό σύστημα για κινητά στον κόσμο, με δισεκατομμύρια ενεργές συσκευές. Αυτό καθιστά το Android μεγάλο στόχο για κακόβουλο λογισμικό. Το πρόβλημα επιδεινώνεται από το γεγονός ότι πολλοί χρήστες δεν προστατεύουν τις συσκευές τους εγκαθιστώντας λογισμικό ασφαλείας και εγκαθιστώντας ενημερώσεις όταν αυτές γίνουν διαθέσιμες.

Ως επί το πλείστον, οι μολύνσεις σε Android προέρχονται από το πρόγραμμα περιήγησής μας στο Διαδίκτυο ή μια εφαρμογή που έχουμε κατεβάσει και εγκαταστήσει στο κινητό μας.



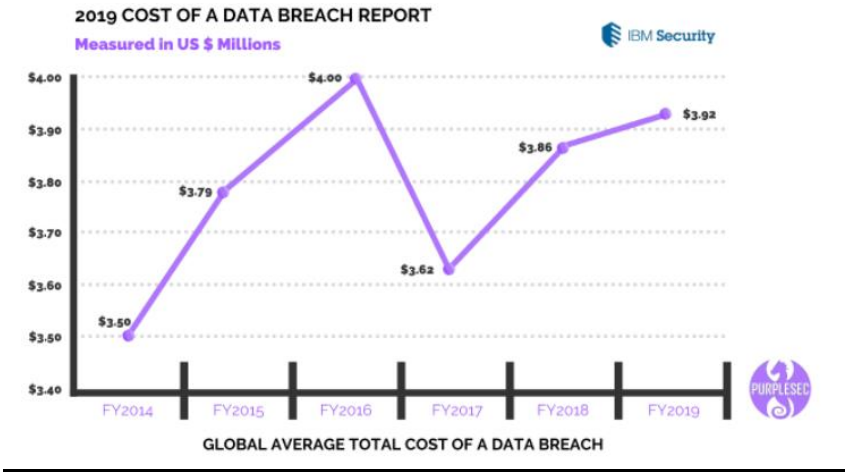
“Το 2021, εντοπίσαμε 3.464.756 κακόβουλα πακέτα εγκατάστασης για κινητά, μειωμένα κατά 2.218.938 σε σχέση με το προηγούμενο έτος. Συνολικά, ο αριθμός των πακέτων εγκατάστασης κακόβουλου λογισμικού για κινητά μειώθηκε περίπου στα επίπεδα του 2019.” (Kaspersky)



Πιθανά αποτελέσματα και κόστη ανάκαμψης από ένα κακόβουλο λογισμικό

Απώλεια δεδομένων: Μία από τις πιο κοινές μορφές βλάβης κακόβουλου λογισμικού είναι η απώλεια δεδομένων. Πολλοί ιοί και trojans θα επιχειρήσουν να διαγράψουν αρχεία ή να σκουπίσουν τους σκληρούς δίσκους όταν ενεργοποιηθούν, αλλά ακόμα κι αν κολλήσετε νωρίς τη μόλυνση, ίσως χρειαστεί να διαγράψετε μολυσμένα αρχεία. Ακόμη χειρότερα, εφόσον οι ιοί μπορεί να μείνουν αδρανείς για κάποιο χρονικό διάστημα, τα αρχεία που έχουν δημιουργηθεί ως αντίγραφα ασφαλείας μπορεί επίσης να έχουν μολυνθεί και να είναι αδύνατη η αποθήκευση.

Κλοπή λογαριασμού: Πολλοί τύποι κακόβουλου λογισμικού περιλαμβάνουν λειτουργίες keylogger, σχεδιασμένες να κλέβουν λογαριασμούς και κωδικούς πρόσβασης από τους στόχους τους. Αυτό μπορεί να δώσει στον δημιουργό κακόβουλου λογισμικού πρόσβαση σε οποιονδήποτε από τους διαδικτυακούς λογαριασμούς του χρήστη, συμπεριλαμβανομένων των διακομιστών email από τους οποίους ο χάκερ μπορεί να εξαπολύσει νέες επιθέσεις. Μια κοινή τακτική που χρησιμοποιείται για τη διάδοση κακόβουλου λογισμικού είναι η αποστολή email σε φίλους και συγγενείς που περιέχουν μολυσμένα αρχεία, καθώς οι χρήστες είναι πιο πιθανό να εκτελούν προγράμματα που τους αποστέλλονται από άτομα που γνωρίζουν.



«Το συνολικό κόστος μιας παραβίασης δεδομένων το 2020 ήταν 3,86 εκατομμύρια δολάρια κατά μέσο όρο.» (IBM 2020, Cost of a Data Breach Report 2020, p. 5, 9)

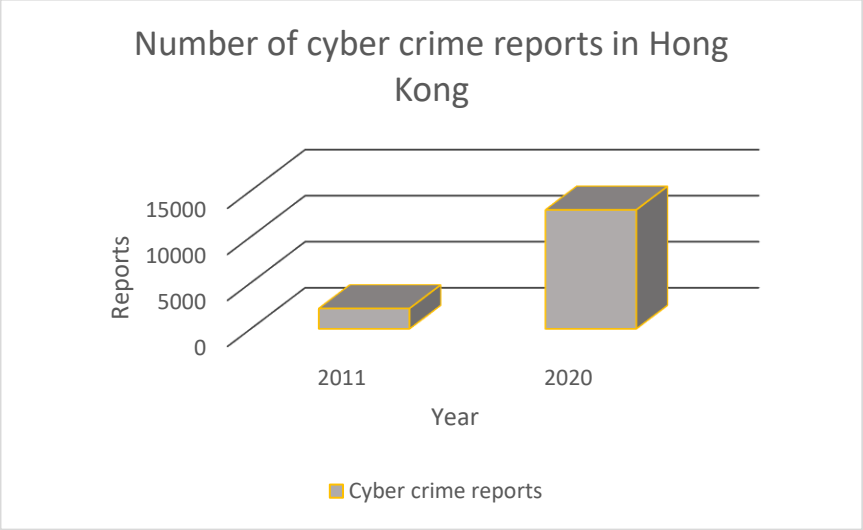
Κανείς δεν μπορεί να είναι πλήρως προετοιμασμένος να πέσει θύμα επίθεσης hacking, αλλά μια γρήγορη αντίδραση είναι ένας κρίσιμος παράγοντας που μπορεί να μειώσει το κόστος σε περίπτωση καταστροφής. Εδώ είναι όπου τα γεγονότα ανάκτησης δεδομένων μπορούν να προσφέρουν μερικές πολύτιμες συμβουλές σχετικά με τη διατήρηση βασικών πληροφοριών μαζί με την εξοικονόμηση χρημάτων.

Η IBM αναφέρει ότι οι εταιρείες με ομάδες αντιμετώπισης περιστατικών που έχουν δοκιμάσει σχέδια IR μπορούν να εξοικονομήσουν έως και 2 εκατομμύρια δολάρια από το συνολικό κόστος των παραβιάσεων.

ΚΕΦΑΛΑΙΟ 2 ΧΟΝΓΚ ΚΟΝΓΚ

Εύρος Απειλής

Την τελευταία δεκαετία, το Hong Kong, είδε τεράστια άνοδο όσο αφορά τα εγκλήματα κατά του κυβερνοχώρου του. Αναλυτικότερα ο αριθμός τέτοιων αναφορών εκτοξεύθηκε από 2.206 το 2011 σε 12.916 το 2020. Στην επιδείνωση αυτή έχει συνδράμει καταλυτικά και η παγκόσμια πανδημία, η οποία ανάγκασε πολλούς εγκληματίες να αναζητήσουν ηλεκτρονικές διόδους. Αυτό ανακλάται από το γεγονός ότι ο αριθμός των περιστατικών το 2020 παρουσίασε αύξηση 55% σε σχέση με την προηγούμενη χρονιά.

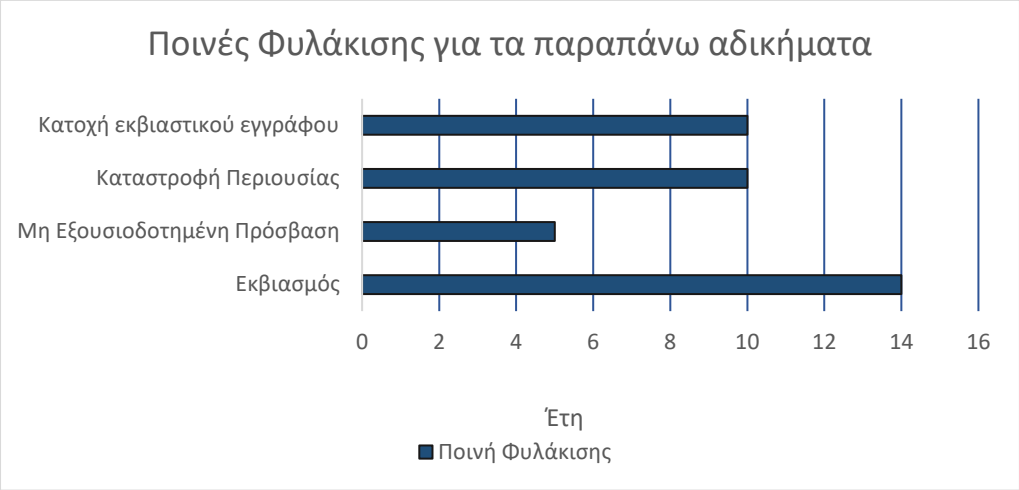


Συγχρόνως, η αξία των εγκλημάτων αυτών πολλαπλασιάστηκε από 148 εκατομμύρια HKD (17.5 εκ. ευρώ) το 2011 σε 2.96 δισεκατομμύρια HKD το 2020 (35 εκ. ευρώ).

Δυνατότητες & Περιορισμοί

Αναφορικά με το ransomware, η ενότητα 23 του Διατάγματος Κλοπής (Κεφάλαιο 210 των Νόμων του Hong Kong) προβλέπει ότι ένα άτομο διαπράττει το ποινικό αδίκημα του εκβιασμού εάν υπό το πρίσμα του να κερδίσει κάτι για τον ίδιο ή για κάποιον άλλον ή για να προκαλέσει απώλεια σε κάποιον, προβεί σε οποιαδήποτε αδικαιολόγητη απαίτηση μέσω απειλών. Πρόσωπα τα οποία κρίνονται ένοχα υπόκεινται σε φυλάκιση για έως και 14 χρόνια. Επιπλέον αξίζει να σημειωθεί ότι, πρόσωπο το οποίο έχει στην κατοχή του ή υπό τον έλεγχό του οποιαδήποτε επιστολή ή γραπτό έγγραφο που υποκινεί εκβιασμό, θα κρίνεται ένοχο του αδικήματος και θα υπόκειται σε φυλάκιση έως και 10 ετών. Παρόλο που η υποενότητα αυτή δεν έχει επικλειθεί ακόμα σε κάποια δικαστική αίθουσα του Hong Kong, θεωρητικά η κατοχή κώδικα ransomware προβάλλοντας κάποια αδικαιολόγητη απαίτηση (χρήματα) μέσω κάποιας απειλής (επανάκτηση αρχείων) θα μπορούσε να συνιστά καταδικαστέο αδίκημα που εμπίπτει στην ενότητα αυτή, διότι ο κώδικας θεωρείτε γραπτό έγγραφο. Βέβαια θα ήταν σημαντική παράλειψη να μην τονιστεί ότι κανένα αδίκημα δεν διαπράττεται εάν το πρόσωπο αποδείξει ότι κατείχε ή έλεγχε το γραπτό χωρίς κακόβουλο σκοπό.

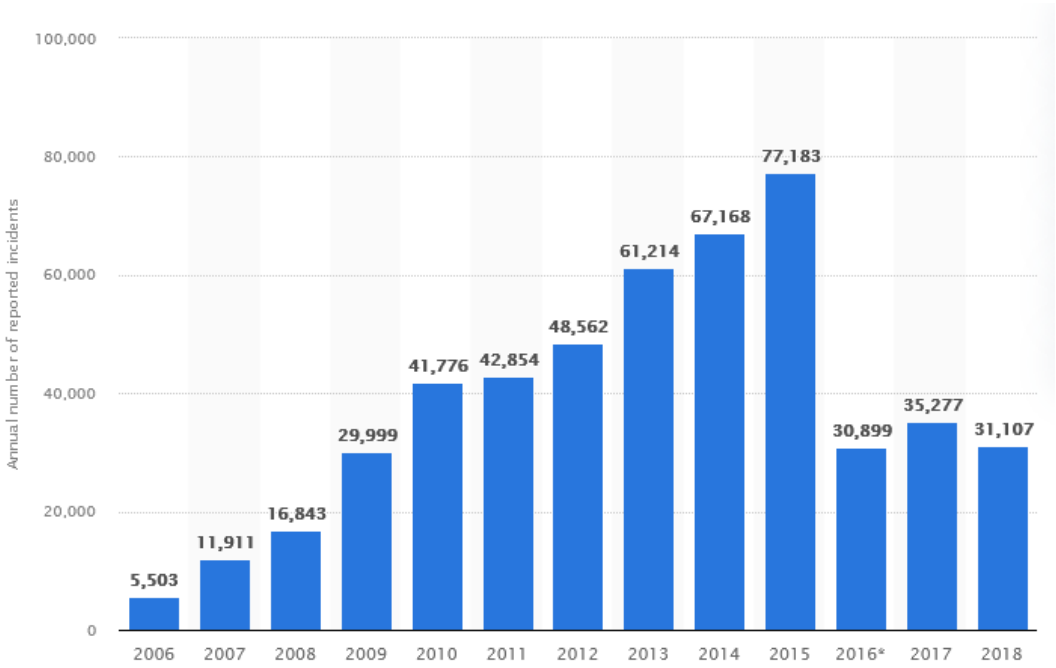
Σύμφωνα με το άρθρο 27Α του Διατάγματος Τηλεπικοινωνιών, είναι ποινικό αδίκημα για ένα άτομο να προκαλέσει εν γνώσει του έναν υπολογιστή να εκτελέσει οποιαδήποτε λειτουργία αποσκοπώντας στην απόκτηση μη εξουσιοδοτημένης πρόσβασης σε οποιοδήποτε πρόγραμμα ή δεδομένα που βρίσκονται στον υπολογιστή. Σε συνάρτηση με αυτό το πλαίσιο, άτομα που καταδικάζονται για δημιουργία ή/και διανομή τέτοιου ιομορφικού λογισμικού μπορούν να έρθουν αντιμέτωπα με ποινή προστίμου επιπέδου 4 ύψους έως 25.000 HKD (3000 ευρώ). Επιπλέον, σύμφωνα με το άρθρο 161 του Διατάγματος για τα Εγκλήματα, που συνήθως χρησιμοποιείται «καθολικά» από τις αρχές σε αδικήματα σχετικά με τον κυβερνοχώρο, άτομο που αποκτά πρόσβαση σε έναν υπολογιστή με σκοπό το ανέντιμο κέρδος για τον ίδιον ή για άλλον (άρθρο 161 (1)(γ)), ή με ανέντιμη πρόθεση να προκαλέσει απώλεια σε άλλον (άρθρο 161 (1)(δ)) διαπράττει ποινικό αδίκημα. Οι ένοχοι αντιμετωπίζουν φυλάκιση έως και 5 έτη. Ωστόσο πρέπει να διευκρινιστεί ότι το άρθρο αυτό δεν εφαρμόζεται όταν δεν έχει προηγηθεί πρόσβαση από έναν υπολογιστή σε έναν άλλον. Παράλληλα το άρθρο 60 του Διατάγματος για τα Εγκλήματα καθιστά ποινικό αδίκημα για ένα άτομο να καταστρέψει ή να βλάψει ιδιοκτησία άλλου. Η ορολογία καταστροφή ιδιοκτησίας περιλαμβάνει την κατάχρηση ενός υπολογιστή που σημαίνει (α) πρόκληση οποιασδήποτε δυσλειτουργίας ακόμα και αν δεν είναι επιβλαβής σε αυτόν, (β) τροποποίηση ή διαγραφή οποιουδήποτε προγράμματος ή δεδομένων του υπολογιστή και (γ) προσθήκη οποιουδήποτε προγράμματος ή δεδομένων στα περιεχόμενα ενός υπολογιστή. Όσοι κρίνονται ένοχοι μπορεί να καταδικαστούν σε κάθειρξη έως και 10 έτη.



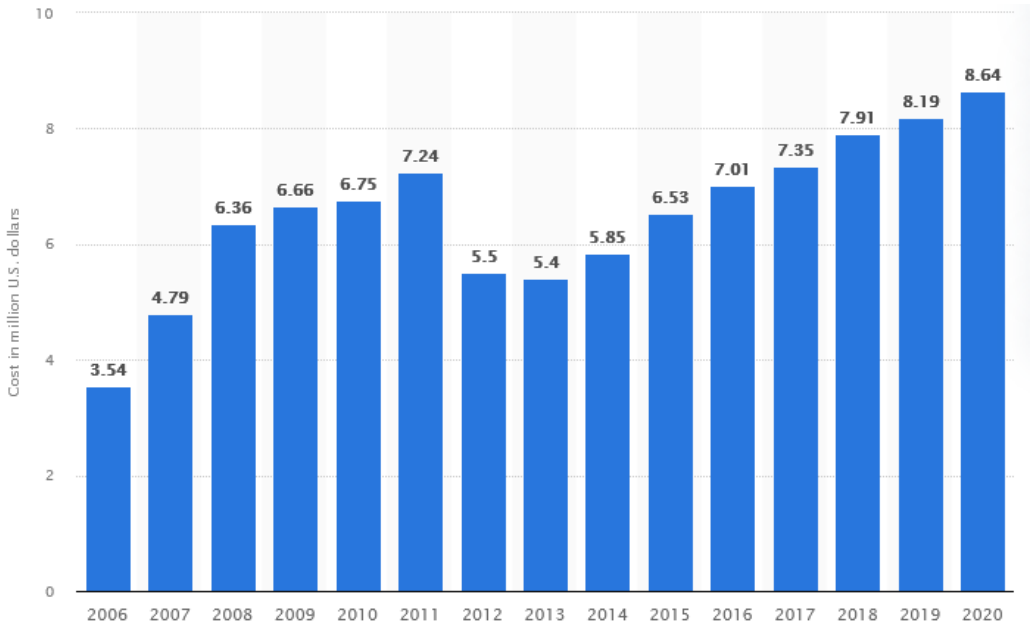
ΚΕΦΑΛΑΙΟ 3 ΗΝΩΜΕΝΕΣ ΠΟΛΙΤΕΙΕΣ ΤΗΣ ΑΜΕΡΙΚΗΣ

Εύρος απειλής

Στις Ηνωμένες Πολιτείες, οι κυβερνοεπιθέσεις προκαλούν ανησυχία εδώ και χρόνια, καθώς έχει αυξηθεί όχι μόνο η συχνότητα των παραβιάσεων δεδομένων, αλλά και η πολυπλοκότητα και οι (οικονομικές) επιπτώσεις τους. Η πλειονότητα των επιθέσεων κακόβουλου λογισμικού παγκοσμίως το 2020 έλαβε χώρα στη Βόρεια Αμερική, με τον αριθμό των αυτοματοποιημένων επιθέσεων bot να υπερβαίνει κατά πολύ αυτόν των επιθέσεων που εκτελούνται από ανθρώπους. Χωρίς αμφιβολία, ως άμεσο αποτέλεσμα της αυξανόμενης αύξησης του ενδιαφέροντος για τα κρυπτονομίσματα, το cryptomining τυγχάνει επίσης να είναι ο κορυφαίος τύπος επίθεσης κακόβουλου λογισμικού. Όχι μόνο οι επιχειρήσεις κινδυνεύουν κάθε χρόνο περισσότερο, αλλά οι δράστες παράγουν επίσης κάθε χρόνο νέες παραλλαγές κακόβουλου λογισμικού, καθιστώντας δυσκολότερη τη σύλληψη.



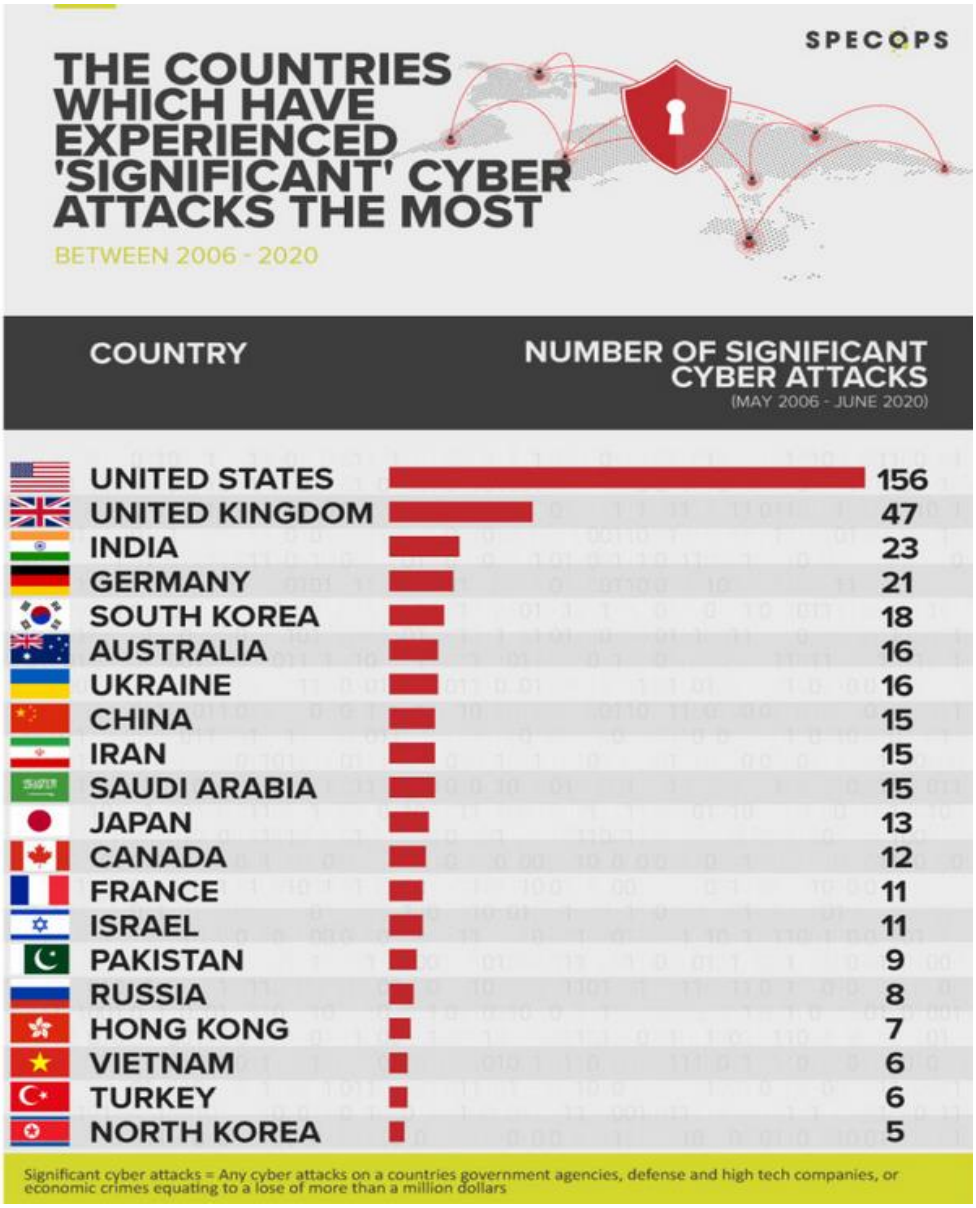
Το 2020, ο αριθμός των παραβιάσεων δεδομένων στις Ηνωμένες Πολιτείες ανήλθε συνολικά σε 1001 περιπτώσεις. Εν τω μεταξύ, κατά τη διάρκεια του ίδιου έτους πάνω από 155,8 εκατομμύρια άτομα επηρεάστηκαν από την έκθεση δεδομένων - δηλαδή την τυχαία αποκάλυψη ευαίσθητων πληροφοριών λόγω της μη επαρκούς ασφάλειας των πληροφοριών.



Επιβεβαιώνεται έτσι η έξαρση των κυβερνοεπιθέσεων στις Ηνωμένες Πολιτείες και την αυξανόμενη ζημία που υφίστανται τα ενωμένα έθνη σε κοινωνικοπολιτικό επίπεδο με οικονομικό και όχι μόνο αντίκτυπο.

Οι Ηνωμένες Πολιτείες, εκτός από τις καθημερινές επιθέσεις απλών χρηστών με υποκλοπές δεδομένων, προσωπικών στοιχείων και ιομορφικά λογισμικά τύπου ransomware,

κατατάσσεται πρώτη σε «σημαντικές» κυβερνοεπιθέσεις σε μεγάλες κυβερνητικές ή οικονομικές δομές και υπηρεσίες.



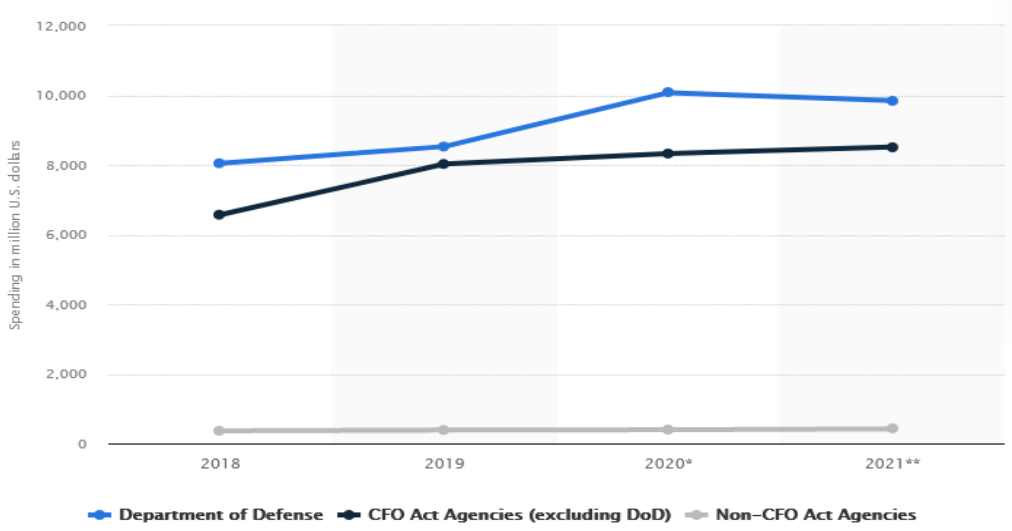
Δυνατότητες & Περιορισμοί

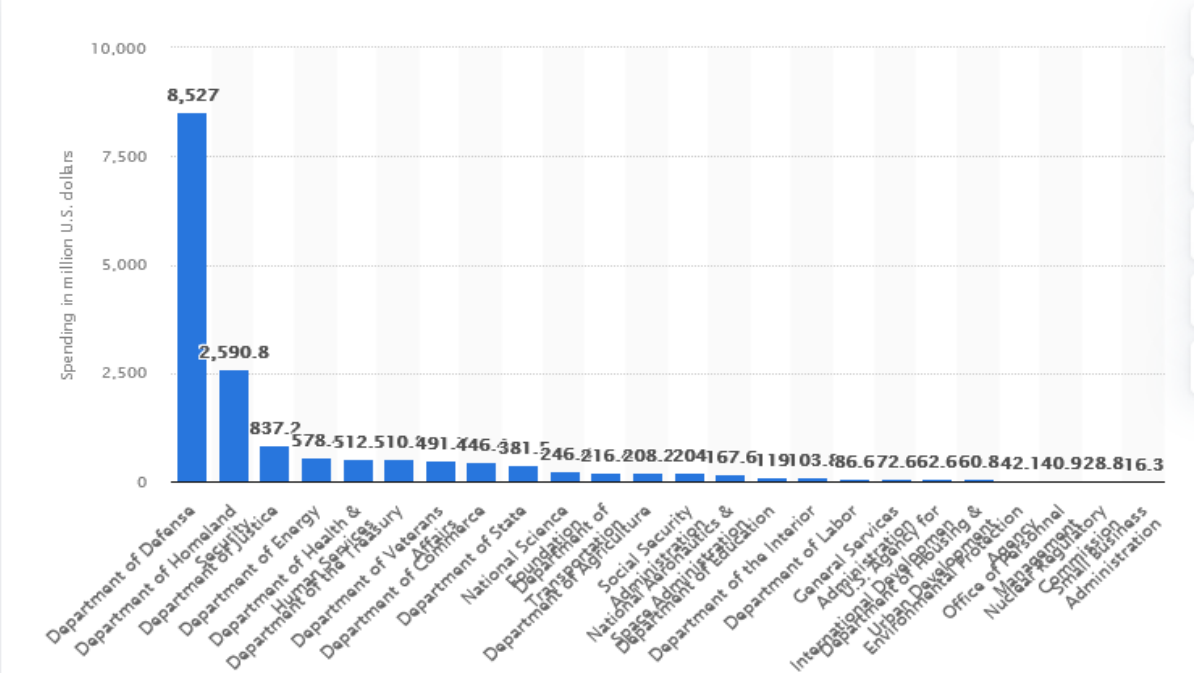
Οι Ηνωμένες Πολιτείες είναι μία από τις χώρες με την υψηλότερη δέσμευση για την ασφάλεια στον κυβερνοχώρο, με βάση τον Παγκόσμιο Δείκτη Ασφάλειας στον Κυβερνοχώρο. Το 2019, οι κυβερνητικές δαπάνες πληροφορικής ανήλθαν σε 88 δισεκατομμύρια δολάρια. Όσον αφορά την κατανομή του προϋπολογισμού, το Υπουργείο Άμυνας (DoD) ξεχωρίζει ως ο κύριος αποδέκτης των ομοσπονδιακών δαπανών για την κυβερνοασφάλεια, καθώς ο οργανισμός είναι υπεύθυνος για την προστασία των Ηνωμένων Πολιτειών τόσο από offline όσο και από online επιθέσεις. Σύμφωνα με το πιο πρόσφατο δόγμα κυβερνοστρατηγικής του Υπουργείου Άμυνας, οι στόχοι του στον κυβερνοχώρο περιλαμβάνουν τη δημιουργία και τη διατήρηση δυνάμεων για τη διεξαγωγή επιχειρήσεων στον κυβερνοχώρο, τη διασφάλιση και την υπεράσπιση των

δεδομένων του Υπουργείου Άμυνας, την προετοιμασία για διασπαστικές και καταστροφικές κυβερνοεπιθέσεις και την ενσωμάτωση κυβερνοεπιλογών και συμμαχιών στα σχέδια. Το 2020, οι Ηνωμένες Πολιτείες κατέλαβαν την πρώτη θέση στον Παγκόσμιο Δείκτη Κυβερνοασφάλειας (GCI) με βαθμολογία 100 μονάδων δείκτη.

Characteristic	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	100	20	20	20	20	20
United Kingdom	99.54	20	19.54	20	20	20
Saudi Arabia	99.54	20	19.54	20	20	20
Estonia	99.48	20	20	20	19.48	20
Korea (Rep. of)	98.52	20	19.54	18.98	20	20
Singapore	98.52	20	19.54	18.98	20	20
Spain	98.52	20	19.54	18.98	20	20
Russian Federation	98.06	20	19.08	18.98	20	20
United Arab Emirates	98.06	20	19.08	18.98	20	20
Malaysia	98.06	20	19.08	18.98	20	20

Τα παρακάτω γραφήματα δείχνουν τις ετήσιες δαπάνες της αμερικανικής κυβέρνησης για την ασφάλεια στον κυβερνοχώρο για τους οργανισμούς του νόμου CFO και τους οργανισμούς που δεν είναι μέλη του νόμου CFO, καθώς και την χρηματική κατανομή δαπανών για την εθνική κυβερνοασφάλεια. Το 2019, η κυβέρνηση των ΗΠΑ δαπάνησε 8,03 δισεκατομμύρια δολάρια ΗΠΑ για την ασφάλεια στον κυβερνοχώρο των οργανισμών του CFO Act, εκτός του Υπουργείου Άμυνας. Το Υπουργείο Άμυνας αντιπροσώπευε το μεγαλύτερο μερίδιο του κυβερνητικού προϋπολογισμού για την ασφάλεια στον κυβερνοχώρο.





Υπάρχουν αρκετοί ομοσπονδιακοί κανονισμοί για την ασφάλεια στον κυβερνοχώρο και αυτοί που υπάρχουν επικεντρώνονται σε συγκεκριμένους κλάδους. Οι τρεις κυριότεροι κανονισμοί για την ασφάλεια στον κυβερνοχώρο είναι ο νόμος του 1996 για τη φορητότητα και τη λογοδοσία της ασφάλισης υγείας (Health Insurance Portability and Accountability Act - HIPAA), ο νόμος Gramm-Leach-Bliley του 1999 και ο νόμος του 2002 για την εσωτερική ασφάλεια, ο οποίος περιλάμβανε τον ομοσπονδιακό νόμο για τη διαχείριση της ασφάλειας των πληροφοριών (Federal Information Security Management Act - FISMA). Οι τρεις κανονισμοί επιβάλλουν στους οργανισμούς υγειονομικής περίθαλψης, στα χρηματοπιστωτικά ιδρύματα και στις ομοσπονδιακές υπηρεσίες να προστατεύουν τα συστήματα και τις πληροφορίες τους. Επιπλέον, οι κανονισμοί δεν διευκρινίζουν ποια μέτρα κυβερνοασφάλειας πρέπει να εφαρμόζονται και απαιτούν μόνο ένα "εύλογο" επίπεδο ασφάλειας. Η ασαφής διατύπωση αυτών των κανονισμών αφήνει πολλά περιθώρια ερμηνείας.

Η στρατηγική του Υπουργείου Άμυνας για τον κυβερνοχώρο:

Τον Απρίλιο του 2015, το Υπουργείο Άμυνας των ΗΠΑ (DoD) δημοσίευσε την τελευταία του στρατηγική για τον κυβερνοχώρο, η οποία βασίζεται στην προηγούμενη στρατηγική του DoD για τη λειτουργία στον κυβερνοχώρο που δημοσιεύθηκε τον Ιούλιο του 2011. Αυτό περιλαμβάνει την προετοιμασία για τη λειτουργία και τη συνέχιση της εκτέλεσης αποστολών σε περιβάλλοντα που επηρεάζονται από επιθέσεις στον κυβερνοχώρο.

Το Υπουργείο Άμυνας περιγράφει τρεις αποστολές στον κυβερνοχώρο:

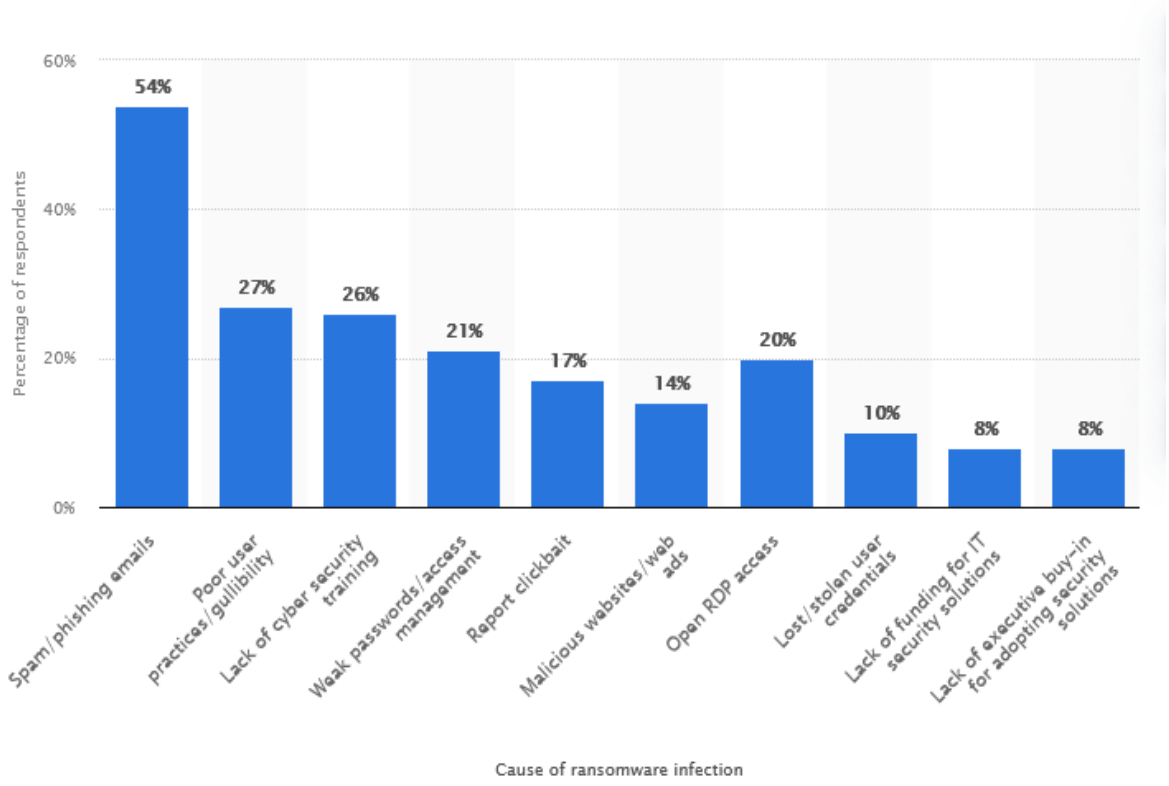
1. Υπεράσπιση δικτύων, συστημάτων και πληροφοριών του DoD.
2. Υπεράσπιση των Ηνωμένων Πολιτειών και των συμφερόντων τους από επιθέσεις στον κυβερνοχώρο με σημαντικές συνέπειες.

3. Παροχή ολοκληρωμένων δυνατοτήτων στον κυβερνοχώρο για την υποστήριξη στρατιωτικών επιχειρήσεων και σχεδίων έκτακτης ανάγκης.

Επιπλέον, η στρατηγική για τον κυβερνοχώρο υπογραμμίζει την ανάγκη να δημιουργηθούν γέφυρες με τον ιδιωτικό τομέα, έτσι ώστε το καλύτερο ταλέντο και η καλύτερη τεχνολογία που έχουν να προσφέρουν οι Ηνωμένες Πολιτείες να είναι στη διάθεση του DoD.

Οι προσωπικές πληροφορίες στις Ηνωμένες Πολιτείες προστατεύονται επί του παρόντος από ένα συνονθύλευμα ομοσπονδιακών νόμων για συγκεκριμένους κλάδους και πολιτειακών νομοθεσιών των οποίων το πεδίο εφαρμογής και η δικαιοδοσία ποικίλλουν. Συνεπώς, η πρόκληση της συμμόρφωσης για τους οργανισμούς που ασκούν επιχειρηματική δραστηριότητα και στις 50 πολιτείες είναι σημαντική.

Στο παρακάτω γράφημα φαίνονται οι πιο συνηθισμένες μέθοδοι μολύνσεων από ιομορφικά λογισμικά και οι πιο συνηθισμένες ευπάθειες συστημάτων.



ΣΥΜΠΕΡΑΣΜΑΤΑ

Συνολικά,

Κυβερνοπόλεμος είναι η χρήση της τεχνολογίας των υπολογιστών για τη διατάραξη των δραστηριοτήτων ενός κράτους ή οργανισμού, ιδίως η σκόπιμη επίθεση σε πληροφοριακά συστήματα για στρατηγικούς ή στρατιωτικούς σκοπούς. Ως μεγάλη ανεπτυγμένη οικονομία, οι Ηνωμένες Πολιτείες εξαρτώνται σε μεγάλο βαθμό από το Διαδίκτυο και, ως εκ τούτου, είναι σε μεγάλο βαθμό εκτεθειμένες σε κυβερνοεπιθέσεις. Ταυτόχρονα, οι Ηνωμένες Πολιτείες διαθέτουν σημαντικές δυνατότητες τόσο στην άμυνα όσο και στην προβολή ισχύος χάρη στη συγκριτικά προηγμένη τεχνολογία και τον μεγάλο στρατιωτικό προϋπολογισμό.

Το Χονγκ Κονγκ βρίσκει την κοινωνία του σε μια ευάλωτη κοινωνικοπολιτική κατάσταση θέτοντας στο στόχαστρο των κακόβουλων χρηστών του διαδικτύου τον οποιοδήποτε χρήστη του. Η νομοθεσία είναι επαρκής για να τιμωρήσει πράξεις κυβερνοεγκλήματος από οποιοδήποτε φυσικό πρόσωπο, αλλά συγκριτικά με την Αμερική δεν υπάρχουν αρκετές υποδομές για να στηρίξουν ένα στιβαρό, και πιο ολιστικό, σύστημα αμύνης.

Αναφορικά με το malware – και γενικά την επικινδυνότητα στο διαδίκτυο - θα μπορούσε να αναρωτηθεί κανείς, θα παύσει σύντομα να ανησυχεί ο μέσος χρήστης του διαδικτύου για το αν θα πέσει θύμα κάποιας κυβερνοαπειλής; Για να σταματήσει ολοσχερώς η κατάσταση αυτή με έναν απόλυτο τρόπο, θα πρέπει να κατασκευαστεί ένα σύστημα το οποίο θα είναι **άθικτο** και θα αντιστέκεται σε κάθε μορφής επίθεση, κοινώς θα είναι κλειστό και σφραγισμένο από το εξωτερικό του περιβάλλον. Τίθεται όμως ένα ηθικό ερώτημα. Ένα τέτοιο σύστημα θα **προωθεί** ή θα **καταστέλλει** την **δημοκρατία** και την **ελεύθερη διακίνηση ιδεών**; Ο σκοπός του θα είναι η **προστασία** των μελών του και του **κοινού καλού** ή η «**φυλάκισή**» τους;

“Malware attacks would not work without the most important ingredient: *you.*”

ΑΝΑΦΟΡΕΣ

Cisco (2022). What is Malware?, Available from: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

CheckPoint (2021). The 5 Most Common Types of Malware, Available from: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/the-5-most-common-types-of-malware/

Malwarebytes. Android Security, Available from: https://www.malwarebytes.com/android-antivirus

Milton Kazmeyer. (2013) Damage From a Malware Intrusion, Available from: https://smallbusiness.chron.com/wont-virus-scan-delete-virus-76542.html

Digintrude. Malwares and it's impact on businesses, Available from: https://www.digintrude.com/malwares-and-its-impact-on-business.html

SecureList by Kaspersky (2021). Mobile malware evolution 2021, Available from: https://securelist.com/mobile-malware-evolution-2021/105876/

BunkMyCell. How many phones are in the world, Available from: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

IBM (2020), Cost of a Data Breach Report 2020, p. 5, 9, Available from: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

Matt Bower, Fai Hung Cheung, Karen Chan, Jeffrey Huang (2021) A guide to Hong Kong's cyber security laws and practices, Available from: https://www.allenovery.com/global/-/media/allenovery/2_documents/news_and_insights/publications/2021/06/a_guide_to_hong_kongs_cyber_security_laws_and_practices_june_2021.pdf

Statista (2019). Number of cyber security incident reports by federal agencies in the United States from FY 2006 to 2018.[online] Available from: https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov

Statista (2021). Annual number of data breaches and exposed records in the United States from 2005 to 2020. [online] Available from: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed

Statista (2020). Average organizational cost to a business in the United States after a data breach from 2006 to 2020 .[online] Available from: https://www.statista.com/statistics/273575/average-organizational-cost-incurred-by-a-data-breach

Specops (2020). The countries experiencing the most 'significant' cyber-attacks. [online] Available from: https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

Statista (2021) Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2020.[online] Available from: https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/

Statista (2020). Cyber security spending of the U.S. government on CFO Act and non-CFO Act agencies from FY 2018 to FY 2021.[online] Available from: https://www.statista.com/statistics/1003402/us-cyber-security-spending-cfo-act-agencies/

Statista (2020). Cyber security spending of the U.S. government on selected government departments in FY 2019. [online] Available from: < https://www.statista.com/statistics/697244/us-government-spending-cyber-security-department/

IT governance, (2018). Data Breach Notification Laws by State.[online] Available from: https://www.itgovernanceusa.com/data-breach-notification-laws#MT

Statista (2020). Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020. [online] Available from: https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection