

Τοπικότητα των Κυβερνοαπειλών: Ιομορφικό Λογισμικό

Βιβλιογραφική εργασία που αναπτύχθηκε στα πλαίσια του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων*.

Η εργασία εκπονήθηκε από τους φοιτητές:

- Νικηφόρος Στάβερης, 3160163
- Κωνσταντίνος Καρλής, 3190077
- Αγγελική Φέκα, 3140290

Ημερομηνία παράδοσης: 25 Απριλίου 2022

Συνολική έκταση βασικού περιεχομένου: 2.497 λέξεις*

*Η συνολική έκταση υπολογίστηκε χωρίς να ληφθούν υπόψιν η συγκεκριμένη σελίδα metadata, ο πίνακας περιεχομένων και οι βιβλιογραφικές πηγές. Οι τίτλοι ενοτήτων και υποενοτήτων έχουν συμπεριληφθεί.

Πίνακας Περιεχομένων

ΚΕΦΑΛΑΙΟ 1: ΤΟ ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΤΟ ΑΝΤΙΚΤΥΠΟ ΤΟΥ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ	3
1.1: Η ΠΕΡΙΠΤΩΣΗ ΤΟΥ RANSOMWARE.....	4
ΚΕΦΑΛΑΙΟ 2: HONG KONG: ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ.....	5
2.1: ΤΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ.....	5
2.2: ΕΠΙΘΕΣΕΙΣ ΙΟΜΟΡΦΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ ΣΤΗΝ ΧΩΡΑ.....	5
2.3: BOTNETS: ΤΟ ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ «ΕΝ ΖΩΗ», ΜΕΣΑ ΑΠΟ ΚΑΚΟΒΟΥΛΑ ΔΙΚΤΥΑ ΠΟΥ ΕΧΟΥΝ ΡΙΖΩΣΕΙ ΣΤΗΝ ΧΩΡΑ.	8
2.4: ΤΟ ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ ΩΣ ΟΠΛΟ ΠΟΛΙΤΙΚΟΥ ΕΚΒΙΑΣΜΟΥ	11
2.5: SMART CITY BLUEPRINT: “NEEDS CYBERSECURITY PLAN”	11
ΚΕΦΑΛΑΙΟ 3: ΗΠΑ: ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ	12
3.1: ΤΑ ΔΕΔΟΜΕΝΑ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ	12
3.2: ΤΟ ΙΣΧΥΟΝ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΪΣΙΟ	14
3.3: ΟΙ ΕΠΙΘΕΣΕΙΣ ΜΕ RANSOMWARE ΣΥΝΕΧΙΖΟΥΝ ΝΑ ΕΞΕΛΙΣΣΟΝΤΑΙ ΚΑΙ ΝΑ ΑΠΑΣΧΟΛΟΥΝ	14
3.4: ΣΗΜΑΝΤΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΣΤΗ ΧΩΡΑ.....	15
ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΠΗΓΕΣ	16

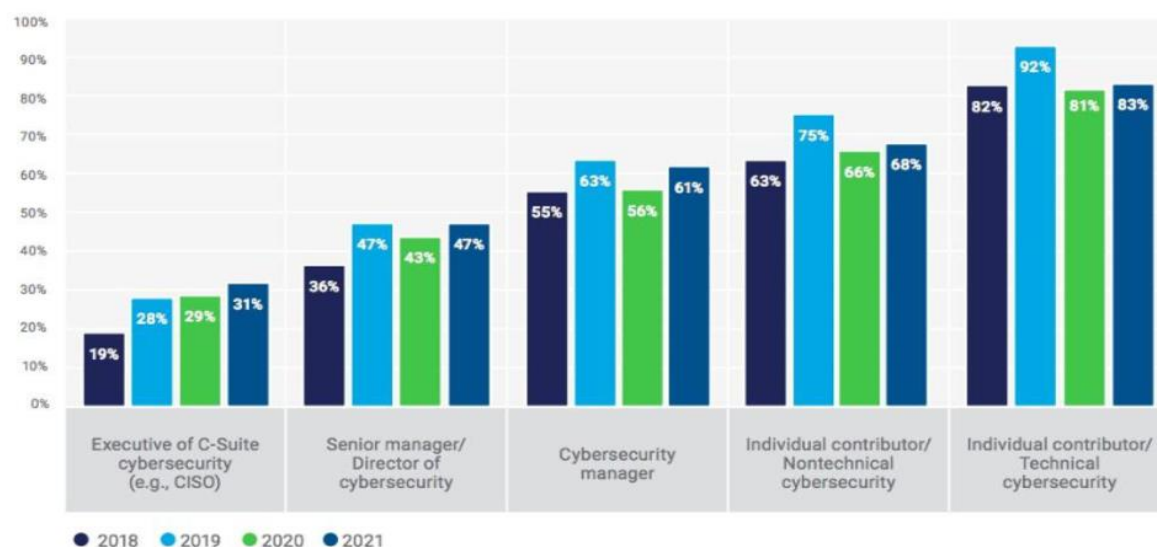
Κεφάλαιο 1: Το Ιομορφικό λογισμικό και το αντίκτυπό του στην Κυβερνοασφάλεια

Τις τελευταίες δεκαετίες παρατηρείται πως το ιομορφικό λογισμικό γίνεται όλο και πιο «δημοφιλές» στον χώρο της κυβερνοασφάλειας. Το malware χρησιμοποιείται πλέον με επιτυχία σε ρόλο όπλου σε επιθέσεις στον κυβερνοχώρο. Γι' αυτό τον λόγο, αντιλαμβανόμαστε πως η συλλογή και η ανάλυση του μπορεί να διαδραματίσει κρίσιμο ρόλο στην ενεργητική άμυνα. Ο προσδιορισμός του στόχου, των δυνατοτήτων, των αδυναμιών καθώς και του εξοπλισμού του αντιπάλου αναμφισβήτητα ενισχύει την στρατηγική άμυνας στον κυβερνοχώρο.[7]

Η ιστορία μας δείχνει πως οι εταιρίες και οργανισμοί δεν έχουν δείξει την απαραίτητη προσοχή και αφοσίωση σε θέματα κυβερνοασφάλειας. Μάλιστα, σύμφωνα με τα λεγόμενα του James Taylor, Διευθυντή Στρατηγικής Ανάπτυξης στο HB και την Ιρλανδία, μόλις το 25% των 100 κορυφαίων εταιριών στο Η.Β κάνουν οποιαδήποτε αναφορά στο απόρρητο και την ασφάλεια στις εκδόσεις τους περί κοινωνικών ευθυνών. Ο ίδιος ανέφερε χαρακτηριστικά πως αν μπορούσε να κατασκευάσει μια λύση «Security culture», θα ανέπτυξε το πιο αποτελεσματικό προϊόν ασφάλειας προς πώληση. Θα υπήρχε δηλαδή πρόοδος μόνο αν οι διάφοροι οργανισμοί αξιολογούσαν τους κινδύνους κυβερνοασφάλειας με το ίδιο σθένος όπως το κάνουν για τους νομικούς, οικονομικούς ή λειτουργικούς.[29]

Στην Έκθεσή της 'Κατάσταση Κυβερνοασφάλειας το 2021' η ISACA διαπίστωσε ότι το 61% των επαγγελματιών στον τομέα της κυβερνοασφάλειας πιστεύει ότι η ομάδα κυβερνοασφάλειας του οργανισμού τους δεν είναι επαρκώς στελεχωμένη. Η υποστελέχωση μεταξύ οργανισμών, συμπεριλαμβανομένων των επιχειρήσεων και της κυβέρνησης, δημιουργεί πίεση στο προσωπικό και συνεπάγεται αυξημένο κίνδυνο από απειλές κακόβουλου λογισμικού.[6]

FIGURE 7: Unfilled Position Reporting for 2018-2021¹¹

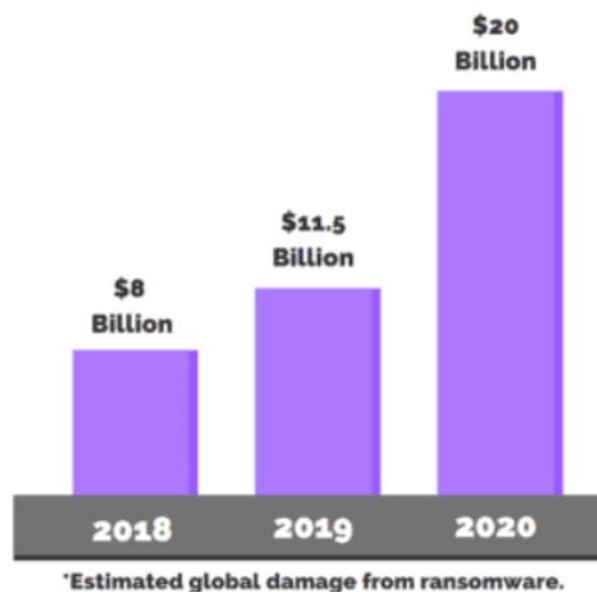


Source: Statistics from ISACA, 2021

Γίνεται πλέον σαφές πως εταιρίες-οργανισμοί ανά χώρα αντιλαμβάνονται διαφορετικά τα ζητήματα προστασίας από malware και γι' αυτό οι ενέργειες τους ποικίλλουν. Απόρροια των παραπάνω είναι η έλλειψη κατάλληλης παρακολούθησης και αντιμετώπισης περιστατικών επιθέσεων κυβερνοασφάλειας. Επιπλέον, στοιχεία από διαφορετικές μελέτες δίδονται και αυτό οφείλεται στο γεγονός ότι οι απαντήσεις βασίζονται στις αντιλήψεις των ερωτηθέντων και όχι στην συνεπή σύλληψη και ανάλυση εμπειρικών δεδομένων. Για παράδειγμα, έρευνες σημειώνουν ότι οι ερωτηθέντες υποτιμούν το κόστος προστασίας με συντελεστή 7/10.[24]

1.1: Η περίπτωση του Ransomware

Όσο τα προβλήματα παραμένουν ανεπίλυτα, τόσο μεγαλώνει και η ζημιά που προκαλείται παγκοσμίως. Χαρακτηριστικό παράδειγμα αποτελεί το Ransomware, ένας ταχύτατα αναδυόμενος τύπος malware που έχει καταστροφικές οικονομικές συνέπειες σε επιχειρήσεις.



Source: Global statistics from purplesec.us

Καθώς οι επιθέσεις με ransomware αποσκοπούν κυρίως στην κατάχρηση προσωπικών δεδομένων, οι εισβολείς κρυπτογραφούν τα δεδομένα και έπειτα τα διαγράφουν εάν δεν πληρούνται οι απαιτήσεις τους, έναντι των οποίων προσφέρουν την αποκρυπτογράφηση τους ως αντάλλαγμα. Εάν η επιχείρηση δεν έχει προνοήσει με αντίγραφα ασφαλείας, συνήθως αναγκάζεται να υποκύψει ρισκάροντας σημαντικά ποσά με κίνδυνο να τα χάσει μαζί με τα δεδομένα, καθώς δεν υπάρχουν εγγυήσεις πως η συμφωνία θα τηρηθεί. [8][15]

Συνεχίζοντας, θα αναλύσουμε διεξοδικά την κατάσταση που επικρατεί σε δυο εκ διαμέτρου αντίθετες χώρες, τις ΗΠΑ και το Χονγκ Κονγκ.

Κεφάλαιο 2: Hong Kong: Ανάλυση κινδύνων

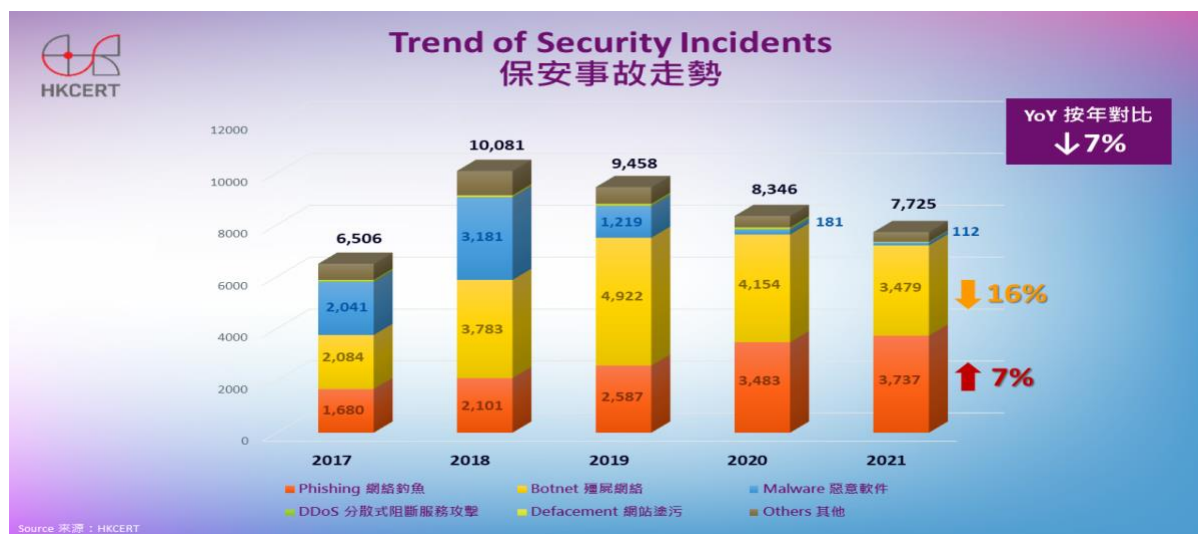
2.1: Τα δεδομένα στην κυβερνοασφάλεια

Το Hong Kong ήταν το πρώτο κράτος στην ευρύτερη περιοχή της Ασίας που το 1996 θέσπισε ολοκληρωμένη νομοθεσία περί απορρήτου προσωπικών δεδομένων (PDPO) καθώς και μια ανεξάρτητη ρυθμιστική αρχή (PCPD) που θα επέβλεπε την εφαρμογή του. Αυτή όμως η πρωτοβουλία που εμπλουτίζεται συνεχώς με ανανεώσεις και εισηγήσεις νέων διατάξεων, εγείρει προβληματισμούς όταν συγκρίνεται με την απουσία αντίστοιχων ενεργειών για την πάταξη εγκλημάτων στον κυβερνοχώρο. Σήμερα εξακολουθεί να μην υπάρχει σαφές νομοθετικό πλαίσιο με μέτρα που στοχεύουν στην καταπολέμηση του κυβερνοεγκλήματος εκτός από μεμονωμένες διατάξεις που αποσκοπούν στην τιμωρία και όχι την πρόληψη των κακόβουλων ενεργειών. Ορισμένες ανεξάρτητες υπηρεσίες έχουν εγκαθιδρυθεί με στόχο την παρακολούθηση και αντιμετώπιση θεμάτων κυβερνοασφάλειας με δύο βασικές, την InfoSec και HKCERT. Οι δράσεις τους είναι σίγουρα ουσιώδεις, όμως το βάρος είναι βαρύ ώστε να το επωμιστούν ολόκληρο υπό την έλλειψη ενός επαρκούς νομοθετικού πλαισίου.[1][30]

Να σημειωθεί πως γειτονικές χώρες όπως η Ταϊβαν και η Κίνα έχουν ήδη προχωρήσει στη θέσπιση ομαδοποιημένων διατάξεων δίνοντας προτεραιότητα στην αντιμετώπιση θεμάτων κυβερνοασφάλειας, από το 2018 και 2020 αντίστοιχα. Μπορεί το HK να είναι πλέον αναπόσπαστο κομμάτι της Κινεζικής επικράτειας, όμως το σύνταγμά του παραμένει ανεξάρτητο από της Κίνας, η οποία δεν έχει το δικαίωμα να επέμβει στην αυτονομία του λόγω της ισχύουσας συνθήκης "One country, two systems". Συνεπώς, η Κινεζική νομοθεσία κυβερνοασφάλειας δεν έχει καμία ισχύ στο σύστημα του HK.

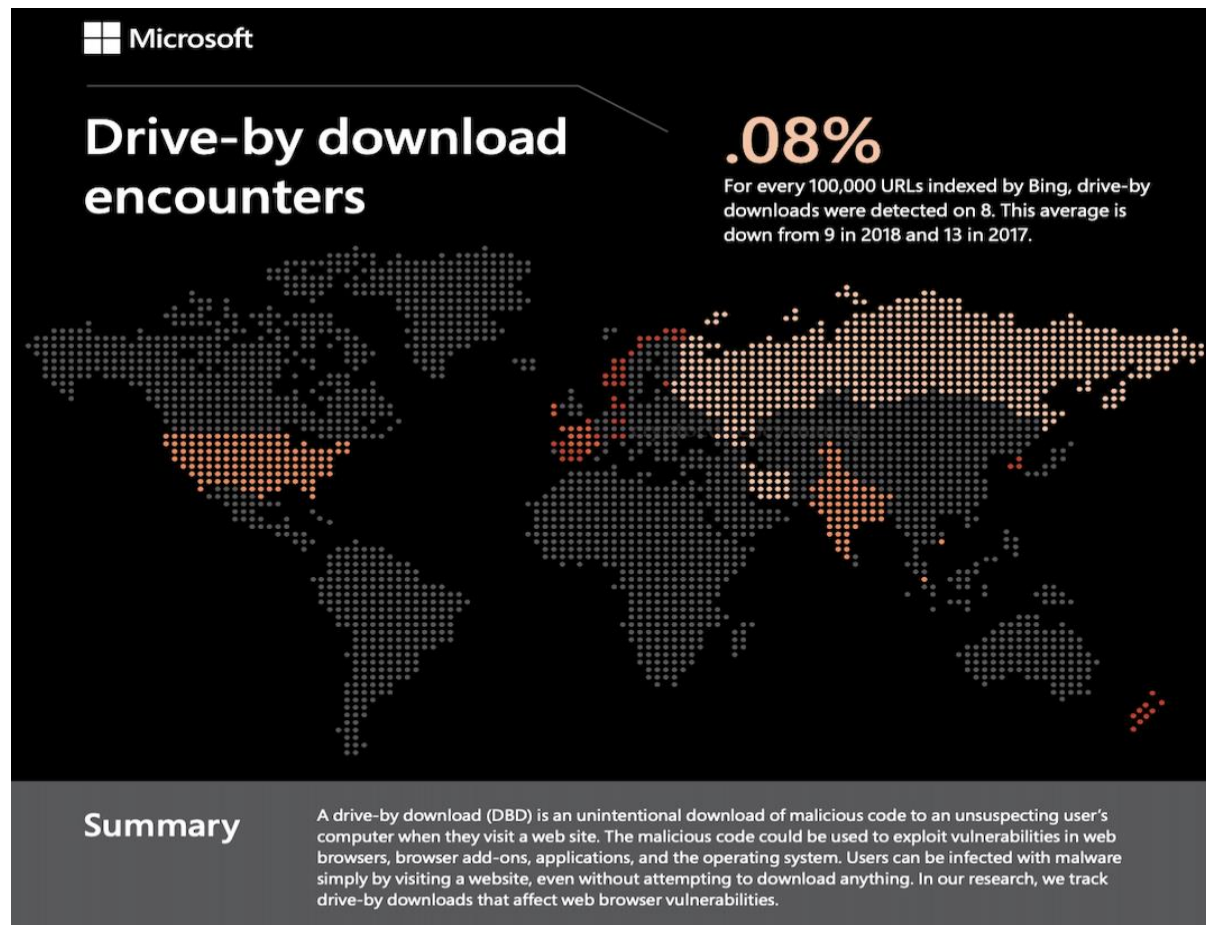
2.2: Επιθέσεις ιομορφικού λογισμικού στην χώρα

Παρ' όλη την αισθητή απουσία μιας συγκροτημένης δομής διατάξεων ικανής να παράσχει οργανωμένη πρόληψη και δράση σε ζητήματα κυβερνοασφάλειας, παρατηρείται πτωτική τάση στις περιπτώσεις επιθέσεων ιομορφικού λογισμικού στο HK:



Όπως παρουσιάζεται στο παραπάνω διάγραμμα που βασίζεται σε στοιχεία και αναφορές όπως έχουν συγκεντρωθεί από την HKCERT[12], η ελάττωση επιτυχών επιθέσεων και μολύνσεων ιομορφικού λογισμικού από το 2018 μέχρι και το 2021 είναι τόσο αισθητή που σχεδόν χαρακτηρίζει μια απειλή που έχει τεθεί υπό πλήρη έλεγχο.

Τα στοιχεία αυτά συνάδουν με την έρευνα που διεξήγαγε η Microsoft το 2019 στα πλαίσια του *Microsoft Security Endpoint Threat Report*[20]:



Average drive-by download encounter rates by country for 2019.
For full details visit: <https://www.microsoft.com/securityinsights>

↑ Highest encounter rates			↓ Lowest encounter rates			↗ Greatest change YoY		
1. Iran	6. Vietnam		1. New Zealand	6. Denmark		1. Taiwan	6. Bulgaria	
2. Russian Fed.	7. France		2. Austria	7. Norway		2. Iran	7. Russian Fed.	
3. Singapore	8. Ireland		3. Switzerland	8. Czech Republic		3. Norway	8. Brazil	
4. United States	9. Hong Kong		4. Korea	9. Spain		4. Indonesia	9. Romania	
5. India	10. Taiwan		5. Belgium	10. Estonia		5. Australia	10. Thailand	

Σύμφωνα με την εν λόγω έρευνα, το Hong Kong φαίνεται να είχε «κατακτήσει» μια θέση στην παγκόσμια αρνητική δεκάδα χωρών με τα περισσότερα ακούσια drive-by downloads ιομορφικού λογισμικού από χρήστες ενώ επιπλέον τοποθετούνταν στην 11^η θέση παγκοσμίως όσον αφορά το malware encounter rate καθώς και στην 9^η θέση της ειδικότερης κατηγορίας ransomware encounter rate σε σχέση με άλλες χώρες της γεωγραφικής έκτασης Asia-Pacific.

Εκ πρώτης όψεως τα στοιχεία αυτά ίσως μαρτυρούν την ευάλωτη θέση του ΗΚ στον χάρτη της κυβερνοασφάλειας η οποία είχε διαμορφωθεί κατά την πάροδο των προηγούμενων ετών μέχρι το 2019. Τα συμπεράσματα της έρευνας προμήνυαν όμως στη πραγματικότητα την θετική εξέλιξη που βλέπουμε μέχρι σήμερα, μια σημαντική δηλαδή πτωτική τάση στην εξάπλωση ιομορφικού λογισμικού στη χώρα. Εξάλλου επισημαίνεται στην ίδια έρευνα με έντονα γράμματα πως το Hong Kong κατέγραψε τότε τις χαμηλότερες περιπτώσεις μολύνσεων malware και ransomware όλων των εποχών του.

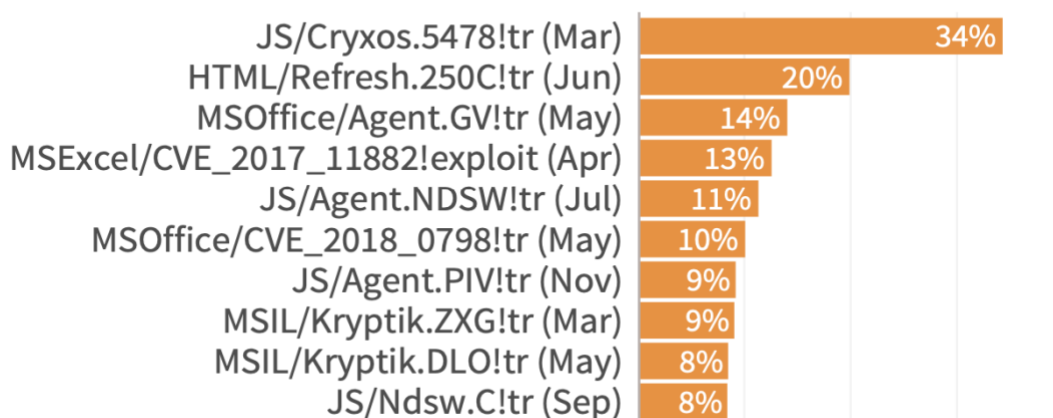
Τα συμπεράσματα αυτά είναι μεν εφησυχαστικά, όμως σε θέματα κυβερνοασφάλειας ο κίνδυνος ελλοχεύει διαρκώς και ο εφησυχασμός δεν πρέπει να γίνει αντιπερισπασμός για τα επόμενα στρατηγικά βήματα. Μπορεί οι καταγεγραμμένες περιπτώσεις επιτυχών μολύνσεων ιομορφικού λογισμικού να φαντάζουν ποσοστιαία αμελητέες, όμως στη πραγματικότητα τα νούμερα «κρύβουν» ένα αδιάκοπο σφυροκόπημα από προσπάθειες για διείσδυση με κακόβουλο λογισμικό ransomware που υφίστανται επιχειρήσεις στο ΗΚ.

Πιο συγκεκριμένα, μεταξύ Απριλίου και Ιουνίου του 2021 καταγράφηκαν κατά μέσο όρο 750.000 περιστατικά το μήνα, όπου επιτιθέμενοι προσπάθησαν να εισβάλουν και να μολύνουν συστήματα επιχειρήσεων με ransomware. Αν και οι περισσότερες από τις επιθέσεις ήταν ανεπιτυχείς, τα υψηλά νούμερα δείχνουν σε έναν «πόλεμο» που μαίνεται καθώς εισβολείς στοχεύουν επίμονα επιχειρήσεις με ανεξάντλητες προσπάθειες μέχρι να καταφέρουν τον στόχο τους.[11][22]

Σε μια τέτοια προσπάθεια μέλη της REvil κατάφεραν να πλήξουν τα υπολογιστικά συστήματα της διαφημιστικής Fimmick που εδρεύει στο ΗΚ και να τα μολύνουν με ransomware τον Σεπτέμβριο του 2021. Η επίθεση είχε ως αποτέλεσμα την πιθανή διαρροή προσωπικών στοιχείων για πάνω από 35.000 άτομα και έθεσε σε κίνδυνο δεδομένα συνεργαζόμενων εταιριών όπως η Coca-Cola China, Nestle HK, L’Oreal HK. [27]

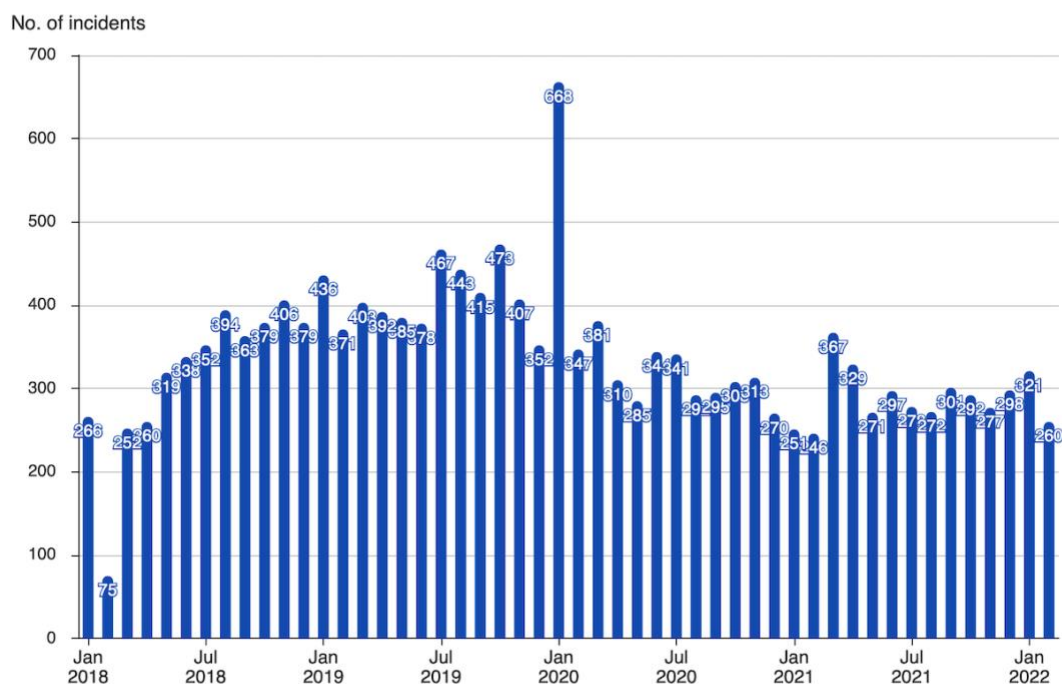
Όσον αφορά τα πιο διαδεδομένα είδη malware που εντοπίστηκαν τους τελευταίους μήνες του 2021 στην ευρύτερη περιοχή Ασίας-Ειρηνικού που εμπεριέχει το ΗΚ, αυτά παρουσιάζονται στο παρακάτω διάγραμμα μαζί με τον μήνα που πρωτοεμφανίστηκαν.[9]

Asia-Pacific



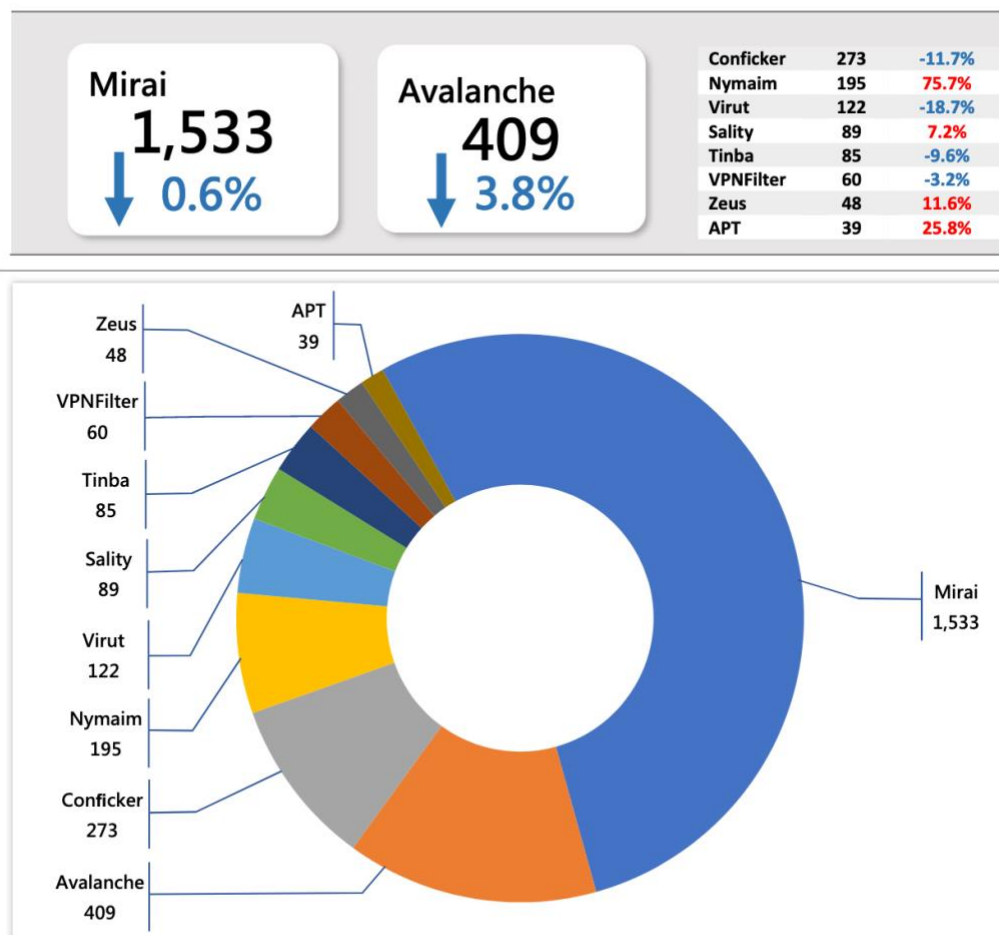
2.3: Botnets: Το ιομορφικό λογισμικό «εν ζωή», μέσα από κακόβουλα δίκτυα που έχουν ριζώσει στην χώρα.

Εκτός από τον κίνδυνο από επιθέσεις με malware, ανησυχία προκαλεί η επίμονη παρουσία των botnets στο ΗΚ. Όπως φαίνεται και από τα στοιχεία του HKCERT, τα περιστατικά όπου ήδη μολυσμένα συστήματα πραγματοποιούν επιθέσεις στον κυβερνοχώρο όντας μέλη του ίδιου δικτύου botnet δεν φαίνονται να φθίνουν.



Οι οικογένειες botnet με την υψηλότερη παρουσία στο ΗΚ είναι μέχρι και το Q4 του 2021 οι: Mirai, Avalanche, Conficker, Nymaim, Virut.[13] Αναλυτικότερα:

Major Botnet Families in Hong Kong Network



* Individual botnet's size is calculated from the maximum of the daily counts of unique IP address attempting to connect to the botnet in the reporting period. In other words, the real botnet size should be larger because not all bots are activated on the same day.

Συγκρίνοντας με αντίστοιχα στοιχεία από το Q1 του 2019[14], διακρίνεται η επίμονη παρουσία των ίδιων οικογενειών, συμπέρασμα που αντικατοπτρίζει ένα μέχρι στιγμής ανεπίλυτο πρόβλημα:

Table 2: Major Botnet Families in Hong Kong Networks











Rank	↑↓	Concerned Bots	Number of Unique IP addresses	Changes with previous period
1	→	Mirai	4,521	9.7%
2	→	WannaCry	989	-18.1%
3	→	Conficker	565	-5.0%
4	→	Virut	305	9.7%
5	→	Avalanche	236	-2.1%
6	→	Sality	123	-16.9%
7	↑	Gamarue	112	11,100.0%
8	↑	ZeroAccess	89	78.0%
9	↓	VPNFilter	87	3.6%
10	↓	Nymaim	73	15.9%

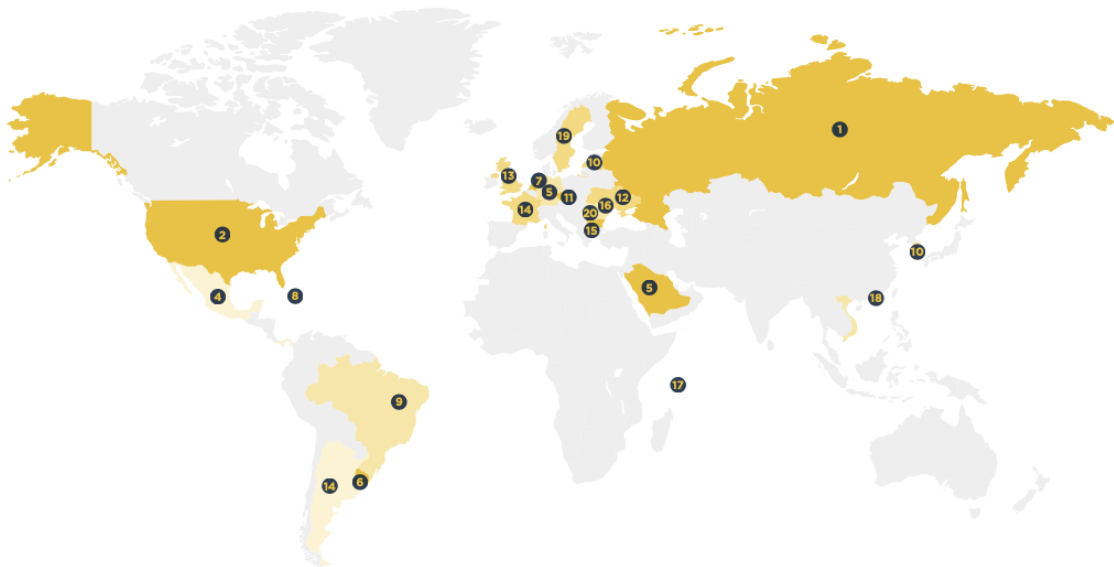
Μάλιστα βάσει της αύξησης σε botnet command and controllers κατά το τελευταίο τρίμηνο του 2021, το Hong Kong κατατάχθηκε στην 18^η θέση παγκοσμίως ως προς τη παρουσία τέτοιων δικτύων και είναι το μοναδικό της περιοχής Ασίας-Ειρηνικού στη λίστα[26]:

Geolocation of botnet C&Cs, Q4 2021 (continued)

Top 20 locations of botnet C&Cs

Rank	Country		Q3 2021	Q4 2021	% Change Q on Q
#1	Russia		381	854	124%
#2	United States		301	384	28%
#3	Germany		170	230	35%
#4	Mexico		182	186	2%
#5	Saudi Arabia		117	180	54%
#6	Uruguay		63	177	181%
#7	Netherlands		273	164	-40%
#8	Dominican Rep		96	110	15%
#9	Brazil		86	92	7%
#10	Latvia		58	69	19%

Rank	Country		Q3 2021	Q4 2021	% Change Q on Q
#11	Czech Republic		40	66	65%
#12	Ukraine		-	64	New Entry
#13	United Kingdom		39	61	56%
#14	France		123	60	-51%
#15	Bulgaria		-	56	New Entry
#16	Moldova		49	50	2%
#17	Seychelles		-	34	New Entry
#18	Hong Kong		-	28	New Entry
#19	Sweden		38	26	-32%
#20	Romania		33	24	-27%



2.4: Το ιομορφικό λογισμικό ως όπλο πολιτικού εκβιασμού

Εκτός από τις κακόβουλες κινήσεις τρίτων κατά επιχειρήσεων και ιδιωτών εντός του ΗΚ, προβληματισμούς εγείρουν μαζικές επιθέσεις που παρατηρούνται και φαίνονται να συνδέονται με πολιτικά κίνητρα αντί για οικονομικά.

Ένα πρόσφατο τέτοιο γεγονός καταγράφηκε τον Νοέμβριο του 2021 όταν αποκαλύφθηκε ότι παράγοντες Κινεζικών συμφερόντων εκμεταλλεύτηκαν αδυναμίες στο λογισμικό του macOS και iOS ώστε να προβούν σε watering-hole επιθέσεις που στόχευαν συσκευές οι οποίες επισκεπτόντουσαν ιστοσελίδες «δημοκρατικού περιεχομένου» προκειμένου να συλλέξουν στοιχεία από τους χρήστες. Στις επιθέσεις χρησιμοποιήθηκε ιομορφικό λογισμικό τύπου OSX.MacMa, OSX.CDDs καθώς και το ειδικά διαμορφωμένο DazzleSpy.[19][32]

Τέτοιες πράξεις κυβερνοεγκλήματος κατά της δημοκρατίας και της ελεύθερης βούλησης είναι και απόπειρες κατά της αυτοδυναμίας του ΗΚ και αποδυνάμωσης του ανεξάρτητου καθεστώτος του και αποτελούν μείζον ζήτημα που πρέπει να αντιμετωπιστεί με την ενίσχυση της κυβερνοασφάλειας.

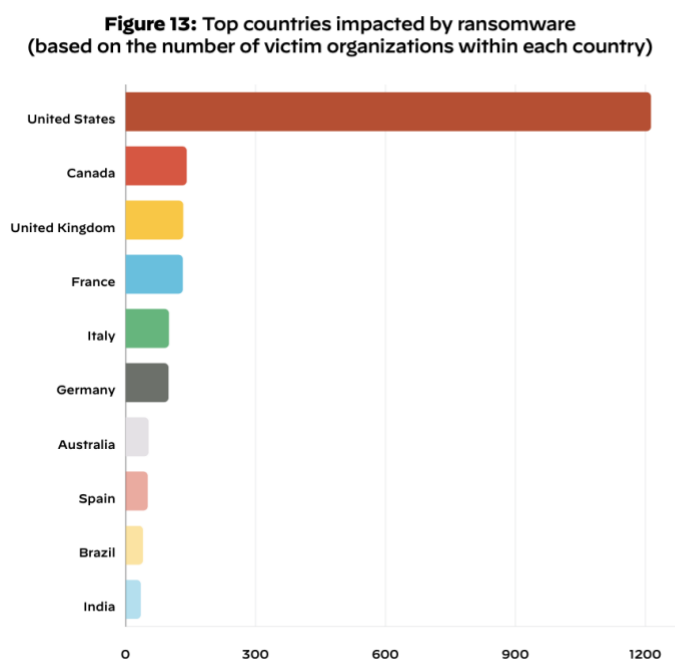
2.5: Smart City Blueprint: “Needs cybersecurity plan”

Το 2017, το ΗΚ δεσμεύτηκε να θέσει σε εφαρμογή το μεγάλο σχέδιο μιας “Εξυπνης πόλης», με μια ολιστική προσέγγιση κατά την οποία όλες οι πτυχές της ζωής στη πόλη θα συνδέονται με τεχνολογικές λύσεις.[18] Το εγχείρημα αν και φιλόδοξο δημιουργεί αμφιβολίες καθώς τα δεδομένα δεν πείθουν ότι η έξυπνη πόλη θα είναι ασφαλής από κακόβουλους εξωτερικούς παράγοντες • το μόνο σίγουρο είναι ότι θα πρέπει να συνδυαστεί με μια ενισχυμένη πολιτική κυβερνοασφάλειας. Επιπλέον, θα χρειαστεί η έμπρακτη συνεισφορά τοπικών παραγόντων με τη συμμετοχή τους σε μια συντονισμένη δράση που θα προωθεί ορθές πρακτικές κυβερνοασφάλειας.

Κεφάλαιο 3: ΗΠΑ: Ανάλυση Κινδύνων

3.1: Τα δεδομένα στην Κυβερνοασφάλεια

Οι κυβερνοεπιθέσεις ιομορφικού λογισμικού στις ΗΠΑ είναι μείζον ζήτημα που προκαλεί ανησυχία καθώς εξελίσσεται δυναμικά και απειλεί τοπικές κυβερνήσεις, επιχειρήσεις και άτομα.[23] Σύμφωνα με την αρμόδια ομοσπονδιακή υπηρεσία CISA, το ransomware αναπτύσσεται συνεχώς και αποτελεί πλέον την κυρίαρχη μορφή απειλής τύπου malware που χρησιμοποιείται στην χώρα. Στον αναλογισμό για την εξέλιξη του ransomware μέχρι το 2022 από το Unit-42 της Palo Alto, η δυσσώιωνα ανοδική πορεία του φαινομένου απεικονίζεται γραφικώς καθώς οι ΗΠΑ κατατάσσονται στην πρώτη θέση των χωρών που έχουν πληγεί περισσότερο από αυτό, με σημαντική διαφορά από τις υπόλοιπες. Μάλιστα υπολογίζεται ότι ο συνολικός όγκος δεδομένων που διέρρευσαν από οργανισμούς της χώρας μετά από επιθέσεις αναλογούν στο 49% των δεδομένων που διέρρευσαν παγκοσμίως.[21]



When we look for trends by country rather than region, the United States was the most severely impacted by data breaches, with U.S. organizations accounting for 49% of the leak site data, followed by Canada and the United Kingdom, accounting for 5% each. Since many ransomware threat actors are highly financially motivated, they often focus on profitable organizations in the United States. That said, ransomware is a global issue; we have observed at least one victim impacted in more than 90 different countries.

49% **5%** **5%**
UNITED STATES CANADA UNITED KINGDOM

Είναι γνωστό ότι σε περιόδους κρίσης πολλοί hackers εκμεταλλεύονται την αναταραχή και την αταξία που επικρατεί, προκειμένου να επωφεληθούν οικονομικά. Η κρίση του COVID-19 έδωσε έτσι ώθηση στην συχνότητα των επιθέσεων ransomware στη χώρα, ενώ οι περιπτώσεις όπου επιχειρήσεις κατέθεσαν λύτρα αυξήθηκαν. Αξιοσημείωτη είναι η περίπτωση όπου η ασφαλιστική-γίγαντας CNA συμμορφώθηκε πληρώνοντας το ποσό-ρεκόρ των 40 εκατομμυρίων δολαρίων μετά από επίθεση της ομάδας Phoenix[4]. Συνολικά, οι επιθέσεις με ransomware αυξήθηκαν κατά 150% σε σχέση με το 2019 και τα ποσά που πλήρωσαν οι επιχειρήσεις σε hackers κατά 300%, σύμφωνα με το Harvard Business Review.[3]

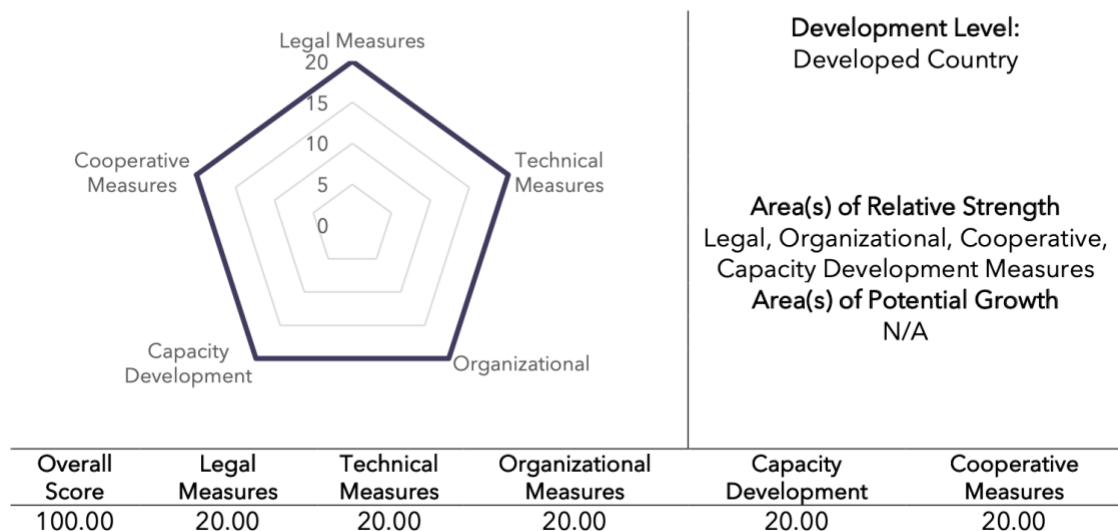
Παρ' όλο που τα παραπάνω στοιχεία συνιστούν μια νέα κρίση στην κυβερνοασφάλεια, η συμμετοχή των ΗΠΑ στην πρωτοβουλία GCI 2020 της ITU φαίνεται πως ανέδειξε κάποια αποτελέσματα που φάνταζαν μάλλον εφησυχαστικά. Συγκεκριμένα, βάσει της κλίμακας CGI που υπολογίζει την βαθμολογία μιας χώρα στον τομέα της κυβερνοασφάλειας με γνώμονα τα 5 βασικά πεδία που την καθορίζουν, οι ΗΠΑ κατατάχθηκαν στην πρώτη θέση ανάμεσα σε συνολικά 194 χώρες.[16]

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

Όπως φαίνεται, την πρώτη θέση συνόδεψε η βαθμολογία του απόλυτου(100) που σημαίνει ότι η χώρα είχε την μέγιστη βαθμολογία και στα 5 βασικά πεδία. Συνολικά παρουσιάζεται στο σχήμα:

United States of America**



Source: ITU Global Cybersecurity Index v4, 2020

Οι υψηλές βαθμολογίες έχουν ίσως βάση, όμως η σιγουριά που εκπέμπουν δεν συνάδει με τη κρίση στη κυβερνοασφάλεια και την «επέλαση» ιομορφικού λογισμικού που πρέπει να περιοριστεί με κατάλληλες αναθεωρήσεις και νέες λύσεις.

3.2: Το ισχύον νομοθετικό πλαίσιο

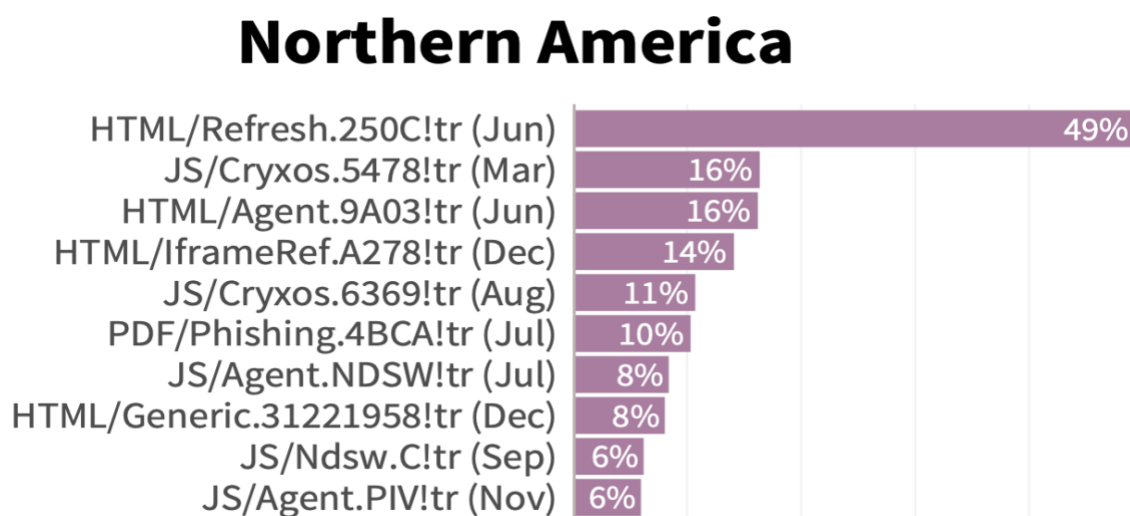
Οι νόμοι για την ασφάλεια στον κυβερνοχώρο των ΗΠΑ είναι αναμφισβήτητα οι παλαιότεροι, πιο ισχυροί και αποτελεσματικοί στον κόσμο, όμως εξακολουθούν να μην εντάσσονται σε ένα ενιαίο πλαίσιο ομοσπονδιακών κανονισμών που διέπει όλους τους τομείς κυβερνοασφάλειας. Έτσι, ο υπάρχον συνδυασμός ομοσπονδιακών και κρατικών κανόνων καθιστά περίπλοκη την υιοθέτηση μιας συγκροτημένης πολιτικής από εταιρίες. Μια εταιρεία που δραστηριοποιείται σε εθνικό επίπεδο και αντιμετωπίζει κάποια παραβίαση δεδομένων, ενδέχεται έτσι να πρέπει να συμμορφωθεί και να δράσει βάσει διαφορετικών απαιτήσεων, ανάλογα με το πως καθορίζεται από την κάθε πολιτεία. [10]

Η θέσπιση μιας ενιαίας εθνικής στρατηγικής που να ξεπερνάει τα όρια της κάθε πολιτείας έχει επιχειρηθεί από διάφορες κυβερνήσεις των ΗΠΑ από το 1990 όμως παραμένει μέχρι σήμερα ένα σχέδιο χωρίς εφαρμογή.[2] Η νέα κρίση ιομορφικού λογισμικού προσθέτει βάρος για την διαμόρφωση ενός τέτοιου σχεδίου και υπενθυμίζει πως οι νόμοι γύρω από την κυβερνοασφάλεια επιδέχονται σημαντικές βελτιώσεις και ως έχουν διαμορφωθεί με τρόπο που τους καθιστά από τους πιο αξιόπιστους παγκοσμίως.

3.3: Οι επιθέσεις με Ransomware συνεχίζουν να εξελίσσονται και να απασχολούν

Το 2021 εξακολουθεί να παρατηρείται δραματική αύξηση σε επιθέσεις malware ενάντια σε κρίσιμες υποδομές, ιδιωτικές εταιρίες και δήμους στις ΗΠΑ. Όταν πρόκειται για ransomware, τα ποσά σε λύτρα που απαιτούνται επίσης αυξήθηκαν και σε ορισμένες περιπτώσεις έφτασαν τα δεκάδες εκατομμύρια δολάρια σε απαιτήσεις που «δικαιολογούνται» από τους πιο περίπλοκους και αποτελεσματικούς αλγορίθμους εκβιασμού που τίθενται πλέον σε ισχύ.

Στο παρακάτω σχήμα διακρίνονται τα πιο διαδεδομένα στελέχη ιομορφικού λογισμικού που συναντώνται το 2021, βάσει στοιχείων της Fortinet[9]:



Η ποσοστιαία αύξηση σε επιθέσεις ransomware συνοδεύεται και από μια ανεπτυγμένη μεθοδολογία που ακολουθούν οι κακόβουλοι παράγοντες. Οι hackers πίσω από τέτοιες επιθέσεις, ανήκουν συνήθως σε οργανωμένα δίκτυα εγκληματικών οργανώσεων, με βαθιά κεκτημένη γνώση των οικονομικών μιας εταιρίας, του κλάδου δραστηριοποίησής της και των συνθηκών που την καθιστούν ευάλωτη σε περίπτωση επίθεσης.

Προβληματισμό προκαλεί το φαινόμενο όπου εγκληματικές ομάδες που δρουν με επιθέσεις ransomware ενώνουν τις δυνάμεις τους και συνεργάζονται υπό τη μορφή «καρτέλ». Σύμφωνα με έρευνα του Analyst1, ένα τέτοιο καρτέλ συντέλεσαν οι ομάδες: Twisted-Spider, Viking-Spider, Wizard-Spider, Lockbit-Gang, τον Μάιο του 2020. Οι ομάδες μοιράζονται κλεμμένα δεδομένα, τακτικές, πληροφορίες και εργαλεία μεταξύ τους ώστε να κάνουν ακόμα πιο αποτελεσματική την δράση τους.[25]

Ένα τέτοιο φαινόμενο απαιτεί τη σύνθεση μιας αντίθετης σύμπραξης που θα σχηματίσει νέες πρωτοβουλίες και δράσεις κατά του οργανωμένου κυβερνοεγκλήματος στη χώρα.

3.4: Σημαντικές περιπτώσεις κυβερνοεπιθέσεων στη χώρα

Η κυβερνοεπίθεση στο Colonial Pipeline το 2021 αποτέλεσε σημείο-σταθμό στα δεδομένα των επιθέσεων με ransomware καθώς και μέσο αφύπνισης. Το αντίκτυπο ήταν τόσο μεγάλο που η καθήλωση του συστήματος διέκοψε την παροχή φυσικού αερίου σε όλη την ανατολική ακτή των ΗΠΑ. Την επίθεση ενορχήστρωσε η ομάδα DarkSide χρησιμοποιώντας darkside:v2.0 ransomware που κατάφερε να λυγίσει το σύστημα τιμολόγησης και το εσωτερικό δίκτυο της εταιρείας οδηγώντας σε εκτεταμένες ελλείψεις σε πολλές πολιτείες. Η εταιρία αναγκάστηκε να πληρώσει λύτρα ύψους 5 εκατομμυρίων δολαρίων υπό την επιτήρηση του FBI και αργότερα κατηγορήθηκε για την μη τήρηση επαρκών μέτρων κυβερνοασφάλειας. Κυβερνητικοί αξιωματούχοι επιβεβαίωσαν πως η επίθεση θα μπορούσε να είχε αποτραπεί αν η εταιρία είχε αναπτύξει αυστηρότερα μέτρα άμυνας, γεγονός που ενισχύει τους προβληματισμούς για το πως οι επιχειρήσεις διαχειρίζονται τα ζητήματα κυβερνοασφάλειας στη χώρα.[5]

Σε μια άλλη συνταρακτική περίπτωση, τον Ιούλιο του 2021 η ομάδα REvil κατάφερε να διεισδύσει στα συστήματα της Kaseya και κατόπιν σε τουλάχιστον 30 MSPs της και να προκαλέσει έτσι την παράλυση των συστημάτων για περίπου 1500 συνεργαζόμενες επιχειρήσεις. Η επίθεση αποτέλεσε σήμα κατατεθέν των όλο και πιο δημοφιλών *supply chain attacks* και μια που διευθετήθηκε αισίως με την συνδρομή του FBI στην ανεύρεση του κλειδιού αποκρυπτογράφησης.[17]

Εξαιτίας των παραπάνω περιπτώσεων, η κυβέρνηση κατέστησε τον βαθμό του εγκλήματος που σχετίζεται με χρήση ransomware ισάξιο με εγκλήματος τρομοκρατίας[25]. Η κρισιμότητα του ζητήματος είναι λοιπόν εμφανής και παρ' όλο που οι ΗΠΑ διαθέτουν ήδη δυνατές υποδομές, επαυξάνεται το συμπέρασμα πως υπάρχει ανάγκη για νέες δραστικότερες λύσεις στην άμυνα κατά του ιομορφικού λογισμικού.

Βιβλιογραφικές Πηγές

- [1] Allen & Overy. (2021), 'A guide to Hong Kong's cybersecurity laws and practices'. Available at: <https://www.allenoverly.com/en-gb/global/news-and-insights/publications/a-guide-to-hong-kongs-cyber-security-laws-and-practices> [Accessed Απρίλιος 2022]
- [2] Baksh, M.(2021) 'US Still Lacks Federal Cyber Strategy After Decades of Attempts', Nextgov, 30 Dec 2021. Available at: <https://www.nextgov.com/cybersecurity/2021/12/us-still-lacks-federal-cyber-strategy-after-decades-attempts/360252/>[Accessed Απρίλιος 2022]
- [3] Brenda R. Sharton, 2021. Ransomware Attacks Are Spiking. Is Your Company Prepared? [online] Available at: <https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared>[Accessed Απρίλιος 2022]
- [4] Chang, B.(2021) 'One of the biggest US insurance companies reportedly paid hackers \$40 million ransom after a cyberattack', Business Insider, 22 May 2021. Available at: <https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5>[Accessed Απρίλιος 2022]
- [5] CISA, 2020. Alert (AA20-049A) Ransomware Impacting Pipeline Operations. [online] Available at: <https://www.cisa.gov/uscert/ncas/alerts/aa20-049a> [Accessed Απρίλιος 2022]
- [6] Cook, S. (2022), 'Malware statistics and facts for 2022', *Comparitech*, 18 February. Available at: <https://www.comparitech.com/antivirus/malware-statistics-facts/>[Accessed Απρίλιος 2022]
- [7] Fanelli, R. (2015), 'On the Role of Malware Analysis for Technical Intelligence in Active Cyber Defense'. In Armistead, L. *Journal of Information Warfare*. Available at: <http://elastic.org/~fche/mirrors/www.cryptome.org/2015/08/nsa-jiw-2015.pdf#page=79>[Accessed Απρίλιος 2022]
- [8] Firch, J. (2021), '10 Cyber Security Trends You Can't Ignore In 2021', *Purplesec*, 29 April. Available at: <https://purplesec.us/cyber-security-trends-2021/>[Accessed Απρίλιος 2022]
- [9] Fortinet. (2022) 'Global Threat Landscape Report - A Semiannual Report by FortiGuard Labs', February 2022. Available at: <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-q1-2022-threat-landscape.pdf>[Accessed Απρίλιος 2022]
- [10] Harshit Agarwal, 2018. A Glance At The United States Cyber Security Laws. [online] Available at: <https://www.appknox.com/blog/united-states-cyber-security-laws> [Accessed Απρίλιος 2022]
- [11] HKB(2021)'Over 750,000 ransomware attacks HK firms monthly', Hong Kong Business, July 2021. Available at:<https://hongkongbusiness.hk/information-technology/news/over-750000-ransomware-attacks-hk-firms-monthly> [Accessed Απρίλιος 2022]

- [12] HKCERT(2022). 'Statistics'. Available at: <https://www.hkcert.org/statistic> [Accessed Απρίλιος 2022]
- [13] HKCERT. (2022) 'Hong Kong Security Watch Report (Q4 2021)', 1 March 2022. Available at: <https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q4-2021> [Accessed Απρίλιος 2022]
- [14] HKCERT. (2019) 'Hong Kong Security Watch Report (Q1 2019)', 30 April 2019. Available at: <https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q1-2019> [Accessed Απρίλιος 2022]
- [15] ico(n.d). Information Commissioner's Office: Ransomware and data protection compliance. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/> [Accessed Απρίλιος 2022]
- [16] ITU Publications (2020) 'Global Cybersecurity Index 2020', Geneva:ITU. Available at: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E/> [Accessed Απρίλιος 2022]
- [17] Kayne J. (2021) 'A "Colossal" Ransomware Attack Hits Hundreds Of U.S Companies, A Security Firm Says', The Associated Press, July 3 2021. Available at: <https://www.npr.org/2021/07/03/1012849198/ransomware-cyber-attack-revil-attack-huntress-labs?t=1650736234113> [Accessed Απρίλιος 2022]
- [18] King, A.(2021) 'Hong Kong Business - Hong Kong can do more in fight against rising cybercrime in financial sector', HK Financial Services Development Council, 4 Oct 2021. Available at: <https://www.fsd.org.hk/en/media/hong-kong-business-20211004-hong-kong-can-do-more-in-fight-against-rising-cybercrime-in-financial-sector>[Accessed Απρίλιος 2022]
- [19] Kovacs, E. (2022) 'New macOS Malware 'DazzleSpy' Used in Hong Kong Attacks', Security Week, 25 Jan 2022. Available at: <https://www.securityweek.com/new-macos-malware-dazzlespy-used-hong-kong-attacks>[Accessed Απρίλιος 2022]
- [20] Microsoft Security Endpoint. (2019) Threat Summary 2019. Available at: <https://news.microsoft.com/wp-content/uploads/prod/sites/570/2020/02/Microsoft-Security-Endpoint-Threat-Summary-2019-Updated.pdf>[Accessed Απρίλιος 2022]
- [21] Palo Alto.(2022) '2022 Unit 42 Ransomware Threat Report', Mar 24 2022. Available at: <https://www.paloaltonetworks.com/resources/research/2022-unit-42-ransomware-threat-report> [Accessed Απρίλιος 2022]
- [22] Protiviti.(2021) 'Security & Privacy Insights – January edition', January 2021. Available at: <https://www.protiviti.com/HK-en/insights/newsletter-security-privacy-january-edition>[Accessed Απρίλιος 2022]

- [23] Purplesec, 2021, '2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends', n.d. Available at: <https://purplesec.us/resources/cyber-security-statistics/> [Accessed Απρίλιος 2022]
- [24] RAND.(2008) 'Cybersecurity Economic Issues', January 2008. Available at: https://www.rand.org/content/dam/rand/pubs/research_briefs/2008/RAND_RB936_5-1.pdf[Accessed Απρίλιος 2022]
- [25] Sjouwerman, S.(2021) 'Ransomware Gangs: Who Are They And How To Stop Them', Forbes, Sep 27 2021. Available at: <https://www.forbes.com/sites/forbestechcouncil/2021/09/27/ransomware-gangs-who-are-they-and-how-to-stop-them/>[Accessed Απρίλιος 2022]
- [26] The Spamhaus Project. (2022) 'Spamhaus Botnet Threat Update: Q4-2021', 20 January 2022. Available at: <https://www.spamhaus.org/news/article/817/spamhaus-botnet-threat-update-q4-2021>[Accessed Απρίλιος 2022]
- [27] The Standard (2021) 'Fimmick ransomware attack puts over 35,000 people's data at risk', The Standard, 21 Oct 2021. Available at: <https://www.thestandard.com.hk/breaking-news/section/4/181793/Fimmick-ransomware-attack-puts-over-35,000-people%27s-data-at-risk>[Accessed Απρίλιος 2022]
- [28] Sungard AS, 2021. Ransomware attacks against U.S government entities: 5 keys observations and takeaways for municipalities. [online] Available at: <https://www.sungardas.com/en-us/blog/ransomware-attacks-on-us-government-entities/> [Accessed Απρίλιος 2022]
- [29] Taylor, J. (2018), 'Cybersecurity: a cultural issue', *Nuvias*, 3 December. Available at: <https://www.nuvias.com/cybersecurity-a-cultural-issue/>[Accessed Απρίλιος 2022]
- [30] Tham, Y. (2021), 'The Privacy, Data Protection and Cybersecurity Law Review: Hong Kong', *The Law Reviews*, 5 November. Available at: <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/hong-kong>[Accessed Απρίλιος 2022]
- [31] Touro College Illinois (2021) 'The 10 Biggest Ransomware Attacks of 2021', 12 November 2021. Available at: <https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php> [Accessed Απρίλιος 2022]
- [32] Winder, D. (2019) 'China Fires 'Great Cannon' Cyber-Weapon At The Hong Kong Pro-Democracy Movement', Forbes, 5 Dec 2019. Available at: <https://www.forbes.com/sites/daveywinder/2019/12/05/china-fires-great-cannon-cyber-weapon-at-the-hong-kong-pro-democracy-movement/?sh=659d4f097c85>[Accessed Απρίλιος 2022]