

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



Πτυχιακή Εργασία

Μελέτη και ανάλυση αγοράς του σκοτεινού διαδικτύου

Δημήτριος Μαντζιώρης

Επιβλέπων : Δρ. Χριστόφορος Νταντογιάν

Επίκουρος Καθηγητής

Ιούνιος 2022

Επιβλέπων :

Χριστόφορος Νταντογιάν, Επίκουρος Καθηγητής,

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Τριμελής επιτροπή :

Εμμανουήλ Μάγκος, Αναπληρωτής Καθηγητής,

Πρόεδρος Τμήματος Πληροφορικής, Ιόνιο Πανεπιστήμιο

Αγγελική Τσώγου, Επίκουρη Καθηγήτρια,

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Χριστόφορος Νταντογιάν, Επίκουρος Καθηγητής,

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

ΑΦΙΕΡΩΣΗ

Στη σύζυγό μου Παρασκευή...

ΠΕΡΙΛΗΨΗ

Σκοπός της εργασίας είναι να περιγράψει την αγορά κακόβουλου ιομορφικού λογισμικού και παράνομων υπηρεσιών στον κόσμο του σκοτεινού διαδικτύου (dark internet), να δώσει μια εικόνα του κόστους αυτών των «προϊόντων» και να εξηγήσει πώς γίνεται η αγορά και χρήση τους.

Σε αυτό το πλαίσιο έγινε προσπάθεια να καταγραφούν τα διαφορετικά είδη του λογισμικού που υπάρχουν προς πώληση στο σκοτεινό διαδίκτυο, να δοθεί μια εικόνα του κόστους για καθένα από αυτά, να παρουσιαστούν ορισμένες περιπτώσεις πραγματικών επιθέσεων που έχουν καταγραφεί αλλά και των οικονομικών επιπτώσεων που έχουν στην πραγματική οικονομία.

Η ίδια η φύση του σκοτεινού διαδικτύου, που είναι ρευστή και διαρκώς μεταβλητή, ορίζει ότι οι παρεχόμενες στην παρούσα εργασία πληροφορίες, ισχύουν σήμερα και μπορεί να μεταβληθούν ή να πάνσουν να ισχύουν στο μέλλον.

Πρόλογος και Ευχαριστίες

Η δημιουργία μιας πτυχιακής εργασίας είναι μια πολύμηνη απασχόληση, η οποία σε κρατάει προσηλωμένο σε ένα αντικείμενο και σε ένα στόχο. Πολλές φορές καταλήγεις να συνδέσαι συναισθηματικά με το αντικείμενο που μελετάς, ακόμα κι αν αυτό έχει μια «σκοτεινή» πλευρά.

Χρειάζεσαι λοιπόν την υποστήριξη πολλών ανθρώπων, για να μπορείς να κρατάς ισορροπίες και να αποστασιοποιείσαι από την μελέτη σου, όταν χρειάζεται. Ταυτόχρονα θα πρέπει να έχεις στήριξη για να επιμένεις και να συνεχίζεις, όταν επέρχεται η κούραση από το ίδιο αντικείμενο ή όποτε η έρευνά σου περιέρχεται σε τέλος.

Στο πλαίσιο αυτό, θα ήθελα να ευχαριστήσω για την αμέριστη βοήθεια και συμπαράστασή του, τον επιβλέποντα καθηγητή μου, κ. Χριστόφορο Νταντογιάν, Επίκουρο Καθηγητή του Τμήματος Πληροφορικής του Ιονίου Πανεπιστημίου.

Περιεχόμενα

Κεφάλαιο Α' Εισαγωγή.....	1
Α.1 Το σκοτεινό διαδίκτυο (Dark Web).....	1
Α.2 Το επιφανειακό, το βαθύ και το σκοτεινό διαδίκτυο.....	2
Α.3 Πως προσπελάζεται το σκοτεινό διαδίκτυο;	3
Α.4 Πως χρησιμοποιείται ο Tor browser	5
Α.5 Onion v.3 διευθύνσεις	6
Α.6 Η χρήση ενός VPN.....	8
Κεφάλαιο Β' Η αγορά στο Dark web	10
Β.1 Αγορά υπηρεσιών	10
Β.2 Αγορά κακόβουλου λογισμικού.....	15
Β.3 Μελέτες για το πλήθος των συναλλαγών στο dark web	18
Β.4 Εξέλιξη κόστους	19
Β.5 Σημεία πώλησης.....	20
Β.6 Η συνολική εικόνα σήμερα	24
Β.7 Η ετήσια εξέλιξη της αγοράς τα τελευταία χρόνια.....	25
Κεφάλαιο Γ' Κατηγορίες κακόβουλου λογισμικού	27
Γ.1 Τραπεζικό κακόβουλο λογισμικό (banking malware)	27
Γ.2 Ευπάθειες πληροφοριακών συστημάτων (vulnerabilities exploit).....	27
Γ.3 Malvertising	31
Γ.4 Ransomware	33
Γ.5 Database leak	40
Γ.6 Botnets – Loaders	43
Γ.7 Cryptojacking	44
Γ.8 Διαρροή δεδομένων του group Conti	44
Κεφάλαιο Δ' Συμπεράσματα.....	49
Δ.1 Τα κρυπτονομίσματα	49
Δ.2 Επικοινωνία και πληρωμή του πωλητή	49
Δ.3 Τρόπος αποστολής.....	51
Δ.4 Αξιοπιστία και εγγυήσεις σε ένα ανασφαλές περιβάλλον.....	52
Βιβλιογραφία	54

Κατάλογος σχημάτων και εικόνων

Εικόνα Α' 0.1: Λειτουργία του δικτύου TOR.....	5
Εικόνα Α' 0.2: Παρέμβαση Europol στο Dark Web.....	9
Εικόνα Β' 0.1: Κατάλογος υπηρεσιών στο Dark Web	11
Εικόνα Β' 0.2: Τιμοκατάλογος υπηρεσιών στο Dark web.....	11
Εικόνα Β'.0.3: Screenshot από το Best Carding World forum	14
Εικόνα Β'.0.4 Αγορά συνδρομής στο KickAss forum	15
Εικόνα Β' 0.5 Πλήθος επιθέσεων ανά μήνα στην Ευρώπη.....	16
Εικόνα Β' 0.6 GUI ηλεκτρονικού καταστήματος στο Dark web	21
Εικόνα Β' 0.7 Ενδεικτική εικόνα hack group.....	22
Εικόνα Β' 0.8 Logon screen σε κάποια σελίδα του Dark web	22
Εικόνα Γ' 0.1 Επιθέσεις λόγω της ευπάθειας Citrix	29
Εικόνα Γ' 0.2 Πώληση υπηρεσιών malvertize στο Dark web.....	33
Εικόνα Γ' 0.3 Πώληση υπηρεσιών ransomware as a service	36
Εικόνα Γ' 0.4 Στιγμιότυπο από υπολογιστή που έχει δεχθεί επίθεση ransomware	36
Εικόνα Γ' 0.5 Το λογισμικό BitPaymer (πρόγονος του DoppelPaymer) σε δράση	38
Εικόνα Γ' 0.6 Φόρουμ διαφημίζει την Linux έκδοση του REvil.....	38
Εικόνα Γ' 0.7 Πληρωμή για αγορά μιας βάσης δεδομένων στο Dark web.....	42
Εικόνα Γ' 0.8 Monero miner που εκτελείται κρυφά μέσω προγράμματος hidec	44

Κατάλογος Πινάκων

Πίνακας Α' 0.1: Μηχανές αναζήτησης στο Dark Web.....	6
Πίνακας Β' 0.1 Ονόματα Hacker forums	13
Πίνακας Β' 0.2 Διευθύνσεις Hack groups	13
Πίνακας Β' 0.3 Διευθύνσεις Hacker forums	14
Πίνακας Β' 0.4 Οι δέκα πιο συχνές απειλές στην Ευρώπη.....	17
Πίνακας Γ' 0.1 Κατανομή κακόβουλων προγραμμάτων το πρώτο τρίμηνο του 2021.	27
Πίνακας Γ' 0.2 Πρόσφατες zero-day exploits.....	30
Πίνακας Γ' 0.3 Τα πιο γνωστά ransomware λογισμικά των τελευταίων ετών.....	37
Πίνακας Γ' 0.5 Τιμές βάσεων που έχουν διαρρεύσει (leaks) τον Ιανουάριο 2022	41
Πίνακας Γ' 0.6 Διευθύνσεις για αγορές βάσεων δεδομένων (leaks)	41

Κεφάλαιο Α'

Εισαγωγή

Ας ξεκινήσουμε με μια σύντομη περιγραφή του κόσμου του Dark web, του υλικού και του λογισμικού που μπορεί κανείς να βρει εκεί, καθώς και του τρόπου πρόσβασης σε αυτό. Είναι άραγε τόσο τρομακτικό μέρος, όσο ακούγεται στον απλό χρήστη; Είναι τόσο δύσκολο να το προσπελάσει και να το εξερευνήσει κάποιος; Θα κινδυνεύσει ο ίδιος ή το υπολογιστικό σύστημα που χρησιμοποιεί από επιθέσεις άλλων χρηστών; Διακυβεύεται η ανωνυμία του;

A.1 Το σκοτεινό διαδίκτυο (Dark Web)

Το σκοτεινό διαδίκτυο, (dark web όπως είναι ευρέως γνωστό) είναι, σύμφωνα με την βικιπαίδεια, ένας ανώνυμος διαδικτυακός ιστός, στον οποίο σκιώδεις χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες. Μπορεί να χρησιμοποιηθεί είτε για θετικούς είτε για αρνητικούς σκοπούς. Αποτελείται από τα αποκαλούμενα σκοτεινά δίκτυα ή darknets, συνήθως δίκτυα επικάλυψης, που προσεγγίζονται με συγκεκριμένο λογισμικό και άδειες και με τη συχνή χρήση πρωτοκόλλων και θυρών που απαντώνται σε μη τυποποιημένες επικοινωνίες. [1], [2]

Στον ιστό αυτό κυριαρχεί η μυστικότητα, η απόκρυψη των IP διευθύνσεων μέσω μεθόδων κρυπτογράφησης, η κάλυψη μέσα από διαδοχικές ανακατευθύνσεις των προγραμμάτων περιήγησης και η χρήση vrn. Παρόλο που η ανωνυμία από μόνη της δεν αποτελεί αδίκημα και δεν διώκεται ποινικά, προσφέρει ένα πέπλο συγκάλυψης σε ανθρώπους ή οργανισμούς που επιδίδονται σε παράνομες δραστηριότητες.

Έχει συνδέσει το όνομά του με κάθε είδους παράνομη δραστηριότητα, όπως εμπόριο ναρκωτικών και όπλων, παιδική πορνογραφία, κακόβουλα προγράμματα υπολογιστών, κυβερνοεπιθέσεις κ.α. Μέχρι και ανάλυση δολοφονίας φυσικών προσώπων έχει αναφερθεί (η οποία αποτράπηκε εγκαίρως), ενώ συνηθισμένες ενέργειες είναι η διάθεση πλαστών χαρτονομισμάτων, πλαστών διαβατηρίων και άλλων εγγράφων ταυτοποίησης, κλεμμένων πιστωτικών καρτών και δεδομένων προσωπικού χαρακτήρα. [3]

Ωστόσο η ανωνυμία λειτουργεί και αντίστροφα, οπότε στις σελίδες του dark web κυριαρχεί η εκατέρωθεν καχυποψία, η μυστικοπάθεια από την πλευρά των «πωλητών» υπηρεσιών και η αμφισβήτηση και ανησυχία από την πλευρά των «αγοραστών» καθώς όλοι προσπαθούν να καλύψουν τα ψηφιακά και τα φυσικά ίχνη τους. Πολλές φορές ο αγοραστής ελέγχει με μικρού κόστους αγορές τον πωλητή, πριν προχωρήσει σε

μεγαλύτερες και πιο ακριβές παραγγελίες. Οι συναλλαγές γίνονται μόνο μέσω κρυπτονομισμάτων, οι κινήσεις των οποίων είναι πιο δύσκολο να ανιχνευθούν και σε καμία περίπτωση μέσω φυσικών νομισμάτων και πραγματικών τραπεζικών λογαριασμών.

Προφανώς ο έλεγχος αυτής της πλευράς του διαδικτύου είναι πιο δύσκολος, γι' αυτό και απαιτεί την συνεργασία της δίωξης ηλεκτρονικού εγκλήματος πολλών χωρών και την καθοδήγηση από διεθνείς οργανισμούς, όπως η Europol. Το ίδιο δύσκολη είναι και η μελέτη των παρεχόμενων προϊόντων και υπηρεσιών, του κόστους αυτών και του προφίλ των πωλητών. Το περιβάλλον του σκοτεινού διαδικτύου είναι ευμετάβλητο, ιστοσελίδες ανοίγουν και κλείνουν διαρκώς, όταν απειλούνται αλλάζουν εξυπηρετητές και γεωγραφική τοποθεσία και όταν κάποια από αυτές τις ιστοσελίδες γίνει πολύ επιτυχημένη συνήθως κλείνει από τις αρχές και οι δημιουργοί της διώκονται.

A.2 Το επιφανειακό, το βαθύ και το σκοτεινό διαδίκτυο

Σε ένα αρκετά κατατοπιστικό άρθρο η εταιρία Kaspersky διαχωρίζει το διαδίκτυο σε τρεις τομείς : το επιφανειακό (surface web), το βαθύ (deep web) και το σκοτεινό (dark web). [4]

Το ανοιχτό ή **επιφανειακό διαδίκτυο** είναι το ορατό σε όλους τους χρήστες κομμάτι του παγκόσμιου ιστού. Το κομμάτι αυτό είναι προσβάσιμο σε όλους, μέσω μηχανών αναζήτησης και αποτελεί μόνο την κορυφή του παγόβουνου, καθώς υπολογίζεται μόνο στο 5% των υπαρχόντων ιστοσελίδων και δεδομένων.

Το μεγαλύτερο μέρος του διαδικτύου, ο κύριος όγκος του παγόβουνου ο οποίος βρίσκεται κάτω από την επιφάνεια, αποτελεί το **βαθύ διαδίκτυο**. Περίπου το 90% των ιστοσελίδων παγκοσμίως ανήκουν σε αυτή την κατηγορία και είναι πρακτικά απρόσιτες μέσω των μηχανών αναζήτησης, καθώς προστατεύονται από κωδικούς, firewalls ή απλά δεν επιτρέπουν την πρόσβαση στα search engine bots. Πρόκειται για απολύτως ασφαλείς ιστοσελίδες, όπως intranets ή databases που προστατεύονται για εταιρικούς λόγους.

Σε αυτό το κομμάτι του βαθέως διαδικτύου περιλαμβάνονται σελίδες με οικονομικό ή τραπεζικό περιεχόμενο, ιατρικά δεδομένα, εταιρικά αρχεία και γενικότερα περιεχόμενο που αφορά ευαίσθητα προσωπικά δεδομένα και δεν επιτρέπεται να είναι ορατό σε μη εξουσιοδοτημένους χρήστες, οπότε δεν είναι και ανιχνεύσιμο. Σε αυτές εντάσσονται σελίδες που περιέχουν :

- Τραπεζικούς λογαριασμούς

- Φορολογικά στοιχεία
- Εταιρικές βάσεις δεδομένων
- Ιατρικούς φακέλους
- Νομικά αρχεία

Οι σελίδες αυτές δεν αποτελούν απειλή για τον μέσο χρήστη, τουναντίον περιέχουν ευαίσθητα δεδομένα που πρέπει να προστατευθούν.

Μόνο ένα μικρό μέρος του παγκόσμιου ιστού είναι μη προσβάσιμο με συμβατικούς browsers και περιέχει παράνομο περιεχόμενο, γι' αυτό και ονομάζεται **σκοτεινό διαδίκτυο**. Μικρότερο κι από το επιφανειακό κομμάτι, έχει τρία βασικά χαρακτηριστικά που το καθιστούν άντρο ανωνυμίας [4] :

- αποκλείει τις μηχανές αναζήτησης
- υποστηρίζει εικονικά κανάλια κυκλοφορίας
- είναι μη προσβάσιμο από τους γνωστούς browsers, χρησιμοποιώντας κρυπτογράφηση και τείχη προστασίας

Η ανωνυμία αυτή δεν εξασφαλίζει βέβαια την εύκολη διάπραξη παράνομων συναλλαγών, ωστόσο δίνει ένα πλεονέκτημα σε όποιον ψάχνει κάτι τέτοιο.

A.3 Πως προσπελάζεται το σκοτεινό διαδίκτυο;

Το σκοτεινό διαδίκτυο είναι ένας όρος που συναντάται από τα μέσα περίπου της δεκαετίας του '90. Στο χώρο αυτό σύχναζαν αρχικά μόνο εξειδικευμένοι χρήστες της τεχνολογίας, είτε κακόβουλοι (χάκερς, κυβερνο-εγκληματίες) είτε καλόβουλοι (όπως αστυνομικοί ή κυβερνητικοί πράκτορες). Με την εξέλιξη της τεχνολογίας όμως και τεχνικές όπως η κρυπτογράφηση, τα Virtual Private Networks (VPN) αλλά και την ανωνυμία που προσφέρει ο Tor browser ο χώρος αυτός έχει μετατραπεί σε ένα μέρος προσβάσιμο σε πολλούς ενδιαφερόμενους χρήστες, στις μέρες μας.

Ο Tor browser («The Onion Routing project») που αναπτύχθηκε στα μέσα της δεκαετίας του '90, παρέχει την δυνατότητα ανώνυμης πρόσβασης σε σελίδες με την κατάληξη .onion Αναπτύχθηκε αρχικά από το NRL (United States Naval Research Laboratory) για να προστατέψει τις online επικοινωνίες των υπηρεσιών ασφαλείας των Η.Π.Α. Ο Tor διατέθηκε σύντομα, το 2004, ως open-source λογισμικό, διαθέσιμο δωρεάν στο κοινό και από τότε συντηρείται και εξελίσσεται από εθελοντές. [5]

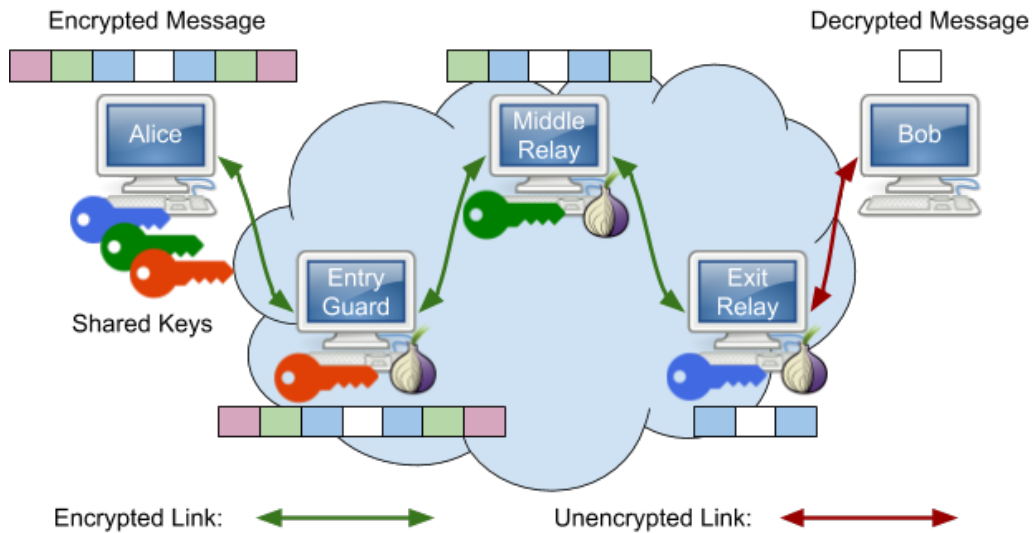
Στην πραγματικότητα, **Tor** ονομάζεται ένα ολόκληρο δίκτυο υπολογιστών. Αποτελείται από διάσπαρτους servers, που ελέγχονται και συντηρούνται κυρίως από

εθελοντές, οι οποίοι καλούνται κόμβοι και είναι διάσπαρτοι σε όλη την υφήλιο. Οι κόμβοι χρησιμοποιούνται ως σημεία αναμετάδοσης των δεδομένων του κάθε χρήστη, ώστε αυτά να δρομολογούνται διαρκώς μέσα στο δίκτυο Tor και να καθίσταται έτσι δύσκολη ως αδύνατη η ανακάλυψη της ταυτότητας του χρήστη. [6]

Το δίκτυο Tor διατηρεί ένα αρχείο όλων των διαθέσιμων κόμβων, ώστε να δρομολογεί τις πληροφορίες μέσω τριών ή περισσότερων από αυτούς. Τα δεδομένα ενός χρήστη που διοχετεύονται μέσω του δικτύου Tor, κατευθύνονται αρχικά σε έναν κόμβο, τον κόμβο – φρουρό, έπειτα σε έναν τουλάχιστον ενδιάμεσο κόμβο και σε έναν κόμβο – εξόδου πριν φτάσουν στον προορισμό τους. Ο browser στέλνει κάθε φορά τα δεδομένα του χρήστη μέσα από ένα τυχαίο μονοπάτι από κόμβους, καθιστώντας πολύ δύσκολη την παρακολούθηση τους.

Το δίκτυο Tor εφαρμόζει επιπλέον κρυπτογράφηση των δεδομένων που διέρχονται των κόμβων, ώστε να εμποδίσει τις ιστοσελίδες να μάθουν την IP διεύθυνση του χρήστη και επομένως την τοποθεσία του ή να υποκλέψουν το περιεχόμενο του μηνύματος. Η κρυπτογράφηση γίνεται κατά την είσοδο των πακέτων πληροφορίας σε κάθε ενδιάμεσο κόμβο του δικτύου. Οι συνηθισμένοι providers διοχετεύουν την κυκλοφορία μόνο μέσω ενός κόμβου, ενώ το δίκτυο Tor δημιουργεί αυξημένη πολυπλοκότητα μέσω των πολλών κόμβων και των πολλαπλών διαδρομών, ώστε να μην επιτρέπει σε εφαρμογές να συγκεντρώνουν δεδομένα των χρηστών, ούτε να βρίσκουν την προέλευσή τους.

Συνοπτικά η διαδικασία είναι η εξής : ο αρχικός κόμβος-φρουρός θα λάβει ένα πλήρως κρυπτογραφημένο μήνυμα από τον χρήστη. Ο δεύτερος κόμβος θα λάβει ένα κρυπτογραφημένο μήνυμα, με την διεύθυνση του αρχικού κόμβου. Ο τελικός κόμβος θα αποκρυπτογραφήσει το μήνυμα αλλά θα έχει την διεύθυνση του δεύτερου κόμβου. Για την απάντηση θα ακολουθηθεί η αντίστροφη διαδρομή, προστατεύοντας έτσι την ανωνυμία του αρχικού χρήστη. [6]



Εικόνα Α' 0.1: Λειτουργία του δικτύου TOR

A.4 Πως χρησιμοποιείται ο Tor browser

Ο Tor browser είναι διαθέσιμος στην ιστοσελίδα <https://torproject.org>, βασίζεται στον Mozilla Firefox browser και παρέχεται δωρεάν. Το περιβάλλον του είναι πολύ απλό και φιλικό στον χρήστη, ενώ με την είσοδο σε αυτόν ζητείται η σύνδεση στο δίκτυο Tor, ώστε να μπορέσει να λειτουργήσει. Πριν από την σύνδεση η ένδειξη είναι offline, ενώ μετά από αυτή μετατρέπεται σε online. Στην σελίδα <https://check.torproject.org/> μπορεί να ελέγξει κάποιος αν όλα έχουν πάει καλά με την σύνδεση του στο δίκτυο Tor και εάν έχει εξασφαλίσει την ανωνυμία του. Στην περίπτωση αυτή, το μήνυμα είναι «Congratulations. This browser is configured to use Tor», ενώ εμφανίζεται και μια εικονική IP address που είναι φυσικά διαφορετική από την πραγματική διεύθυνση του χρήστη.

Η απλή χρήση του είναι απολύτως νόμιμη, στις περισσότερες χώρες του κόσμου. Σε ορισμένες όμως, όπως η Κίνα, δεν επιτρέπεται η ανώνυμη περιήγηση, επομένως μπλοκάρεται όλη η κυκλοφορία των Tor πακέτων. Στην συγκεκριμένη περίπτωση, ο έλεγχος της κυκλοφορίας γίνεται κυρίως στα επίπεδα IP/TCP όπου το ονομαζόμενο *μεγάλο τείχος της Κίνας* (great firewall of China) προσπαθεί να αποτρέψει έναν χρήστη από το να επικοινωνήσει με τον αρχικό κόμβο-φρουρό του δικτύου Tor. Οι προσπάθειες των ειδικών του Tor για την παράκαμψη αυτής της απαγόρευσης επικεντρώνονται στο *επίπεδο εφαρμογής* (application layer) και τη χρήση κάποιων πρόσθετων transport protocols, όπως το scramble suit, ώστε να μην επιτρέψουν στο firewall να ανακαλύπτει τους κόμβους – φρουρούς του δικτύου με probing attacks.

Το επόμενο βήμα είναι η εύρεση μιας μηχανής αναζήτησης η οποία επιτρέπει την εύρεση ιστοσελίδων που παρέχουν πρόσβαση σε κακόβουλο λογισμικό. Προφανώς αυτό δεν είναι και τόσο εύκολο, λόγω της μη καταλογογράφησης τέτοιων σελίδων στις συνηθισμένες μηχανές αναζήτησης. Οι σελίδες αυτές δεν έχουν τις συνηθισμένες καταλήξεις .org ή .com στο URL τους αλλά την κατάληξη .onion και φυσικά δεν είναι καθόλου εύκολο να τις ανακαλύψει κανείς. [7]

Σύμφωνα με την ίδια ιστοσελίδα, υπάρχουν μηχανές αναζήτησης που καταλογογραφούν σελίδες με κατάληξη .onion και επιτρέπουν την αναζήτηση στο dark net, όπως οι μηχανές NotEvil, Candle, Ahmia και Torch. Επιπλέον υπάρχουν οι SearX, Tor66, OnionCenter, Phobos. Μία άλλη επιλογή για όποιον ενδιαφέρεται για το dark web είναι η χρήση των /r/deepweb, /r/onions, και /r/Tor στο Reddit, όπου μπορεί να βρει κάποιος ομάδες συζήτησης και να ζητήσει συμβουλές και οδηγίες.

Πίνακας Α' 0.1: Μηχανές αναζήτησης στο Dark Web

Search Engine name	Onion link
Phobos	http://phobosxilamwgcg75xt22id7aywkzoi6q6rfl2flipcqoc4e4ahima5id.onion/
Ahmia.fi	http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibso4csyd.onion/
DuckDuckGo	https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion
Tor66	http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfxc2e5mxih34iid.onion.dog/
Onion Center	http://5qqr1c7hw3tsqokkqifb33p3mrlpnleka2bjg7n46vih2syngnb6ycid.onion.ly/
Deep Search	https://search7tdrcvri22rieiwgi5g46qnwsesvnuqbav2xakhezv4hjzkkad.onion.pet/
Tor Dex	http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onion/
GDark	http://zb2jtkhnbvhkya3d46twv3g7lkobi4s62tjffqmafjibixk6pmq75did.onion/gdark/search.php
Grams	http://grams64rarzrk7rzdaz2fbb7lehcyi7zrrf5kd6w2uoamp7jw2aq6vyd.onion/
Haystak	http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpfxid.onion/
MetaGer	http://metagerv65pwclop2rsfzg4jwowpavpwd6grhhldvgsswvo6ii4akgyd.onion/

A.5 Onion v.3 διευθύνσεις

Οι διευθύνσεις Version-2 έπαψαν να υποστηρίζονται από τον TOR browser στα τέλη Οκτωβρίου 2021, μετά από 15 ολόκληρα χρόνια. Η νέα μορφή των διευθύνσεων είναι μεγαλύτερη από την προηγούμενη έκδοση (έχουν μεγαλύτερο μήκος) και θεωρείται

ασφαλέστερη από αυτή. Η αλλαγή σε Version-3 έγινε για λόγους καλύτερης κρυπτογράφησης των διευθύνσεων.

Για παράδειγμα, η νέα διεύθυνση v.3 της σελίδας «OnionLinks» είναι:

<http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqknwwqtyd.onion/>

ενώ η «παλιά» v.2 της σελίδας αναζήτησης DuckDuckGo είναι:

<https://3g2upl4pq6kufc4m.onion/>

Όπως φαίνεται παραπάνω, οι διευθύνσεις v.3 έχουν 56 χαρακτήρες πριν την κατάληξη .onion, ενώ οι παλιές v.2 διευθύνσεις είχαν μόλις 16 χαρακτήρες. Αυτό γίνεται επειδή πρέπει να περιέχουν ένα ολόκληρο δημόσιο κλειδί κι όχι μόνο το hash ενός δημόσιου κλειδιού, όπως συνέβαινε με την προηγούμενη έκδοση. Ο κυριότερος λόγος για αυτή την αλλαγή έχει να κάνει με τον *κατάλογο κρυμμένων υπηρεσιών* (hidden service directory – HSDir), ο οποίος είναι υπεύθυνος για την δρομολόγηση προς μια συγκεκριμένη .onion διεύθυνση, όπως το DNS system είναι υπεύθυνο για την δρομολόγηση στις υπόλοιπες διευθύνσεις. [8]

Για να προστατέψει την ιδιωτικότητα των χρηστών του Tor, το HSDir είναι ένα καταναμημένο hash table, που παράγεται από όλους τους κόμβους που επεξεργάζονται ένα HSDir flag. Στην v.2 που ίσχυε μέχρι τώρα, όλα τα δεδομένα του HSDir βρίσκονται σε μορφή απλού κειμένου (text) πράγμα που σημαίνει ότι κάθε κόμβος θα μπορούσε να μάθει ένα σημαντικό ποσοστό των ενεργών .onion υπηρεσιών (σελίδων) κάθε μέρα.

Στην v.3 χρησιμοποιείται κρυπτογράφηση και key derivation για να λυθεί το πρόβλημα. Αφού η ίδια η διεύθυνση είναι ένα ολόκληρο δημόσιο κλειδί, όλα τα δεδομένα μπορούν να είναι κρυπτογραφημένα. Οι κόμβοι μπορούν βέβαια να αποκρυπτογραφήσουν τα δεδομένα, χρησιμοποιώντας το κλειδί που περιέχεται στην .onion διεύθυνση. Ωστόσο θα πρέπει να διαπραγματευτούν με το HSDir ρωτώντας πληροφορίες για κάποια .onion διεύθυνση, γεγονός που θα τους επέτρεπε βέβαια να συγκεντρώσουν και πάλι μεγάλο πλήθος διευθύνσεων καθημερινά. Στην v.3 όμως αυτό αποτρέπεται με την χρήση key derivation που παράγει ημερησίως διαφορετικό κλειδί (blinded public key).

Έτσι ο κάθε κόμβος δεν ρωτάει το HSDir για την διεύθυνση facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion αλλά παράγει αυτόματα ένα αναγνωριστικό συνδυάζοντας την παραπάνω διεύθυνση και την

τρέχουσα ημερομηνία, οπότε ρωτάει για αυτό το blinded public key, στο παράδειγμά μας είναι ek4gJEtlHmwwadLvMNG7tYx/lJuJN1zQl6pMVkGmAcM. [8]

Για λόγους επιβεβαίωσης και για να προφυλάξουν τον χρήστη από εκπλήξεις, οι περισσότερες από τις σελίδες .onion αναγράφουν σε κάποιο σημείο τους ή στο φόντο της αρχικής σελίδας, την νέα v.3 διεύθυνσή τους. Προτρέπουν τους επισκέπτες να επιβεβαιώνουν ότι ταιριάζει με αυτό που βλέπουν στην γραμμή διευθύνσεων, ώστε να είναι σίγουροι ότι βρίσκονται στην σωστή σελίδα και όχι σε κάποια που την μιμείται.

A.6 Η χρήση ενός VPN

Η χρήση Εικονικού ιδιωτικού δικτύου (Virtual Private Network, VPN) δεν είναι υποχρεωτική για πρόσβαση στο dark web, προτείνεται όμως καθώς προσθέτει ένα ακόμη βήμα στην εξασφάλιση ανωνυμίας και απόκρυψης της IP διεύθυνσης του χρήστη.

Οι υπηρεσίες αυτές προσφέρονται σε λογικές τιμές (που ξεκινούν ακόμα και από τα 4 \$ το μήνα, για διετή σύμβαση) από αρκετές αξιόπιστες εταιρίες σε όλο τον κόσμο. Τα πλεονεκτήματα ενός καλού VPN είναι λίγο – πολύ γνωστά, [9]

- ασφαλής κρυπτογράφηση των δεδομένων
- απόκρυψη IP διεύθυνσης
- ασφαλής μεταφορά δεδομένων
- πρόσβαση σε τοπικό περιεχόμενο και παράκαμψη των γεωγραφικών περιορισμών

Ωστόσο η χρήση ενός VPN για παράνομες δραστηριότητες, μπορεί πάντα να προκαλέσει την περιέργεια των αρχών και να στρέψει τις έρευνές τους προς κάποιον συγκεκριμένο πάροχο. Τέτοιο παράδειγμα είναι η κατάσχεση του VPNlab.net και ο τερματισμός των υπηρεσιών του, τον Ιανουάριο 2022. Η κατηγορία ήταν ότι η συγκεκριμένη υπηρεσία χρησιμοποιούνταν συστηματικά για την υποστήριξη σοβαρών εγκληματικών πράξεων, κυρίως επιθέσεις ransomware.

Η υπηρεσία αυτή, η οποία είχε ξεκινήσει την λειτουργία της από το 2008, μπήκε στο στόχαστρο των αρχών όταν διαπιστώθηκε ότι πάρα πολλές έρευνες για παράνομες δραστηριότητες στο dark web κατέληγαν σε χρήστες της. Η ίδια η υπηρεσία διαφημιζόταν στο dark web, πολλές επιθέσεις ransomware ξεκινούσαν από χρήστες της αλλά και διακίνηση μεγάλου όγκου κακόβουλου λογισμικού γινόταν μέσω του VPNlab.net, σύμφωνα με την Europol. Στα πλαίσια λοιπόν της πράξης EMPACT, οι συνεργαζόμενες αρχές αποφάσισαν να κλείσουν την υπηρεσία αυτή. [10]



Εικόνα Α' 0.2: Παρέμβαση Europol στο Dark Web

Επομένως η χρήση ενός VPN μπορεί να εξασφαλίζει την ανωνυμία του χρήστη για οποιαδήποτε δραστηριότητα, ο ίδιος ο εξυπηρετητής της υπηρεσίας όμως μπορεί να μπει υπό παρακολούθηση, σε περιπτώσεις που μεγάλος όγκος παράνομων δραστηριοτήτων περνάει από αυτόν. Ένα ποιοτικό VPN θα πρέπει να προστατεύει όσο μπορεί την ιδιωτικότητα του χρήστη, κυρίως αποκρύπτοντας την IP διεύθυνσή του, τόσο από τον ISP του όσο και από τρίτους.

Επίσης θα πρέπει να σβήνει τα δικτυακά ίχνη του, σβήνοντας το ιστορικό, τις αναζητήσεις και τα cookies. Τα cookies θα πρέπει να κρυπτογραφούνται, ώστε να μην μπορούν να διαβαστούν οι προσωπικές πληροφορίες του χρήστη. Ένα άλλο χαρακτηριστικό των ποιοτικών VPN είναι η δυνατότητα να τερματίζουν κάποια προεπιλεγμένα – από την χρήση – προγράμματα, σε περίπτωση απρόβλεπτου τερματισμού της ασφαλούς σύνδεσης.

Κεφάλαιο Β'

Η αγορά στο Dark web

Ο χώρος του σκοτεινού διαδικτύου χρησιμοποιήθηκε κατά κόρον για αγορά και πώληση παράνομων αντικειμένων και υπηρεσιών. Θα μας απασχολήσουν εδώ τα προϊόντα λογισμικού (software) και υλικού (hardware) που προσφέρονται μόνο εδώ, όντας παράνομα και απαγορευμένα στις υπόλοιπες νόμιμες αγορές. Ποια είναι (καταγραφή), τι ισχυρίζονται οι δημιουργοί τους ότι κάνουν (λειτουργία) και πόσο χρεώνονται (κοστολόγηση). Στους τρεις αυτούς άξονες θα απαντήσει το τρέχον κεφάλαιο.

B.1 Αγορά υπηρεσιών

Ως υπηρεσίες στον συγκεκριμένο χώρο μπορούμε να ορίσουμε τις ενέργειες που θα κάνει κάποιο άτομο ή μια ομάδα, κατά παραγγελία και προς όφελος του αγοραστή, αφού πρώτα λάβει την κατάλληλη αμοιβή. Τα άτομα διαφημίζονται ως hackers και οι ομάδες ως Hack groups, ενώ προσφέρουν τις υπηρεσίες τους με συγκεκριμένους τιμοκαταλόγους.

Οι υπηρεσίες αυτές μπορεί να είναι :

- Email and Facebook hacking, installing trojans, Small DDoS (250 EUR) (μικρές δουλειές σύμφωνα με τους πωλητές, όπου υποκλέπτεται ο κωδικός email ενός ατόμου ή μιας εταιρίας, εγκαθίστανται Trojans σε υπολογιστές ή servers εταιριών, διεξάγονται επιθέσεις άρνησης υπηρεσίας)
- ruining people, espionage, website hacking, DDoS for big websites (500 EUR) (μεσαίου μεγέθους δουλειές όπου γίνεται συνήθως «δολοφονία χαρακτήρα» ενάντια σε άτομα ή μικρές εταιρίες, κατασκοπία, καταστροφή ιστοσελίδων)
- Hijacking a website completely for a huge time (1000 to 100000 EUR) (μεγάλες και πιο ακριβές δουλειές που περιλαμβάνουν πειρατεία ιστοσελίδας για μεγάλο χρονικό διάστημα, ώστε να προβάλλονται διαφημίσεις ή να ανακατευθύνονται οι χρήστες σε άλλες ανεπιθύμητες για αυτούς σελίδες)

Rent a Hacker	http://2ogmr1fzdthwkez.onion/
Hacking is an Art	http://vb75uj2ap3hyaya.onion/
Hack Group	http://hackerijqhmq6jb.onion/

If you don't know how to access the dark web may go to our must-read page.

To visit any onion website you need to download the tor-browser.

There are lots of more links available you can find using [dark web search engines](#) or our dark web links directory.

How much they charge for there services?

Small Jobs: Email and Facebook hacking, installing trojans, Small DDOS (250 EUR).

Mediums Jobs: ruining people, espionage, website hacking, DDOS for big websites (500 EUR).

Large Jobs: Hijacking a website completely for a huge time (1000 to 100000 EUR).

Εικόνα Β' 0.1: Κατάλογος υπηρεσιών στο Dark Web

Επίσης :

- Απομακρυσμένος έλεγχος κινητού του θύματος
- Hacking σε συγκεκριμένους κοινωνικούς λογαριασμούς Facebook, Twitter, Instagram, Reddit
- Απόκτηση πρόσβασης σε προσωπικούς ή εταιρικούς υπολογιστές και λογαριασμούς, με απώτερο σκοπό την υποκλοπή δεδομένων
- Hacking σε gaming servers

Product	Price	Quantity
Remote control the phone of someone else, most new models supported	700 USD = 0.01127 ₿	1 X Buy now
Facebook and Twitter account hacking	500 USD = 0.00805 ₿	1 X Buy now
Other social network account hacks, for example reddit or instagram	450 USD = 0.00725 ₿	1 X Buy now
Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.02899 ₿	1 X Buy now
DDOS for protected websites for 1 month	900 USD = 0.01450 ₿	1 X Buy now
DDOS for unprotected websites for 1 month	400 USD = 0.00644 ₿	1 X Buy now

Εικόνα Β' 0.2: Τιμοκατάλογος υπηρεσιών στο Dark web

Οι υπηρεσίες που απευθύνονται στο –όχι και τόσο - ευρύ κοινό που εισέρχεται στο dark web, έχουν να κάνουν συνήθως με εφαρμογές που χρησιμοποιούνται ευρέως, όπως email, social media, κινητά τηλέφωνα. Διαφημίζονται λοιπόν υπηρεσίες όπως η παρακολούθηση

κάποιου μέσω του κινητού τηλεφώνου του, η ανάκτηση χαμένου κωδικού κάποιου ατόμου σε Facebook, Instagram, YouTube αλλά και η κλοπή του κωδικού άλλου ατόμου, η κλοπή του ηλεκτρονικού πορτοφολιού κάποιου άλλου (crypto-currency portfolio), ακόμα και η παρέμβαση σε τραπεζικές υπηρεσίες όπως διαγραφή χρέους προς την τράπεζα ή αύξηση ορίου πιστωτικής κάρτας.

Οι ιστοσελίδες που παρουσιάζουν αυτές τις υπηρεσίες έχουν σύγχρονο και φιλικό προς τον χρήστη περιβάλλον, όπου προβάλλονται διαφημίσεις (όπως αυτές που φαίνονται στις παραπάνω εικόνες) για υπηρεσίες hacking, τιμοκατάλογοι, οδηγίες για αγορά κρυπτονομισμάτων που θα χρησιμοποιηθούν για πληρωμή, οδηγίες επικοινωνίας. Το κόστος ξεκινάει από 250\$ και φτάνει μέχρι 1100\$. Ο χρόνος διεκπεραίωσης εξαρτάται από το είδος της υπηρεσίας και τις ιδιαίτερες απαιτήσεις του κάθε πελάτη.

Υπάρχουν τιμοκατάλογοι για πιο εξειδικευμένες υπηρεσίες και ίσως για πιο απαιτητικούς πελάτες. Έτσι προσφέρεται ως υπηρεσία η πρόσβαση σε συγκεκριμένο υπολογιστή, προσωπικό ή εταιρικό, πρόσβαση σε βάση δεδομένων με προσωπικό λογαριασμό και κωδικό, αδρανοποίηση ιστοσελίδας ή server μέσω DDOS, έλεγχος ασφαλείας υπολογιστικών συστημάτων μέσω επίθεσης κ.α.

Phishing service for 150\$ «I will social engineer any target and hack the mailbox, save emails and setup mail forward to any address of your choosing. If the SE is not successful I cancel order. Otherwise, no refund.»	Υπηρεσία ψαρέματος για 150\$ Θα χειραγωγήσω (κοινωνική μηχανική) οποιονδήποτε στόχο και θα χακάρω το mailbox, θα υποκλέψω τα emails του και θα κάνω προώθηση σε άλλη διεύθυνση της επιλογής σας. Αν η χειραγωγήση αποτύχει θα ακυρώσω την παραγγελία. Σε άλλη περίπτωση δεν υπάρχει επιστροφή χρημάτων.																											
1 BTC = 58772.62USD 1 XMR = 247.15USD																												
SPEAR PHISHING SERVICE   <table border="1"> <tr> <td>Price</td> <td>:</td> <td>150.00 USD</td> </tr> <tr> <td>Seller</td> <td>:</td> <td>montecrypto</td> </tr> <tr> <td>Seller location</td> <td>:</td> <td>Worldwide</td> </tr> <tr> <td>Ships to (seller)</td> <td>:</td> <td>Worldwide</td> </tr> <tr> <td>Ships to (product)</td> <td>:</td> <td>Worldwide</td> </tr> <tr> <td>Category</td> <td>:</td> <td>Hacks</td> </tr> <tr> <td>Quantity in stock</td> <td>:</td> <td>997</td> </tr> <tr> <td>Dead drop</td> <td>:</td> <td>No</td> </tr> <tr> <td>Availability</td> <td>:</td> <td>Available</td> </tr> </table>		Price	:	150.00 USD	Seller	:	montecrypto	Seller location	:	Worldwide	Ships to (seller)	:	Worldwide	Ships to (product)	:	Worldwide	Category	:	Hacks	Quantity in stock	:	997	Dead drop	:	No	Availability	:	Available
Price	:	150.00 USD																										
Seller	:	montecrypto																										
Seller location	:	Worldwide																										
Ships to (seller)	:	Worldwide																										
Ships to (product)	:	Worldwide																										
Category	:	Hacks																										
Quantity in stock	:	997																										
Dead drop	:	No																										
Availability	:	Available																										

Εκτός από τις μεμονωμένες ιστοσελίδες, υπάρχουν πολλά forums στα οποία μπορεί να επικοινωνήσει κάποιος πελάτης με ένα hack group ή τα μέλη του hack group μεταξύ τους. Στις πλατφόρμες αυτές λαμβάνουν χώρα συζητήσεις για τρέχουσες ή μελλοντικές κυβερνο-

επιθέσεις, διατίθενται δωρεάν tutorials για hacking ή ανταλλάσσονται πληροφορίες για ευπάθειες και κενά ασφαλείας λογισμικών.

Μπορεί να φαίνεται παράδοξο, εκ πρώτης όψεως, να παραδίδονται μαθήματα hacking, ωστόσο είναι ένας συνηθισμένος τρόπος για να στρατολογούνται και να εκπαιδεύονται νέα μέλη στα group. Τα μέλη αυτά έχουν ελάχιστη ή μέτρια εμπειρία αρχικά, μπορούν όμως να φανούν πολύ χρήσιμα μακροπρόθεσμα.

Πίνακας Β' 0.1 Ονόματα Hacker forums

Φανερά forums	Forums που έχουν γίνει γνωστά στο ευρύ κοινό	Antichat, Blackhackerz, Blackhat World	Διαφημίσεις υπηρεσιών (π.χ. μίσθωση DDOS επιθέσεων), συζητήσεις για διοργάνωση επιθέσεων
Κλειδωμένα forums	Forums που έχουν κλείσει από τις αρχές	Darkode, Shadowcrew, Cardersmarket	Tutorials, δωρεάν exploits συνήθως παλιότερης τεχνολογίας (SQLi, BlackPOS)
Ενεργά forums	Ενεργά και προσβάσιμα forums	OpenSC, Ashiyane, Reverse4you, Exelab	Συζητήσεις για κενά ασφαλείας, για γνωστές ή άγνωστες ευπάθειες, για νέου τύπου επιθέσεις

Μία μεγάλη και ουσιαστική διαφορά ανάμεσα στα forums αυτά και τις μεμονωμένες ιστοσελίδες είναι η γλώσσα. Ενώ οι ιστοσελίδες είναι γραμμένες στα Αγγλικά ώστε να είναι κατανοητές από ένα μεγάλο πλήθος χρηστών από διαφορετικές χώρες, πολλά από τα forums χρησιμοποιούν αποκλειστικά άλλες γλώσσες, όπως Ρωσικά, Αραβικά, Ινδικά κ.α.

Παρακάτω φαίνονται οι .onion διευθύνσεις ορισμένων hack groups, που είναι ενεργά σήμερα. Σε κάποια η επικοινωνία γίνεται μέσω της δημιουργίας λογαριασμού, γεγονός που δεν είναι και τόσο ασφαλές για τον πελάτη, ενώ σε άλλα γίνεται μόνο μέσω ασφαλούς email.

Πίνακας Β' 0.2 Διευθύνσεις Hack groups

Όνομα group	Διεύθυνση .onion
Dark Web Hackers	http://prjd5pmbug2cnfs67s3y65ods27vamswdaw2lnwf45ys3pjl55h2gwqd.onion/
Tor Hacker services	http://zkllmhuxmf3u6lh4cl3lueyoxjvxooenwv7k2wrhatyhw2mknfjtnrid.onion/
Duckers	http://3qpzilhobdujzsoyjxggbedxvgvg6tczdev2s4siqkoky764v6yg6vad.onion/
InstaHacks	http://3w45xure3vzfcra4cawymoxaqwelinqtq2zzq4ixo3rypyrnxxwyqcnad.onion/
Black Hackers	http://wvqwx2pvn54vodexdspb45nto5brtuomdibcdc5xk22kijnjjsseov6kid.onion/black-hackers.htm

Οι διευθύνσεις ορισμένων forums τα οποία είναι ενεργά σήμερα φαίνονται στον παρακάτω πίνακα. Οι κατηγορίες συζητήσεων δεν επικεντρώνονται μόνο στην αγορά προϊόντων αλλά έχουν ευρύτερο ενδιαφέρον.

Πίνακας Β' 0.3 Διευθύνσεις Hacker forums

Όνομα group	Διεύθυνση .onion
Kickass forum	http://qaoxsnp5cjjxbv7duyo7e52dvsagxxveq2gm4w5b7vwr3ecpxatonid.onion/
Raddle forum	http://c32zjeghpc5tj3kb72pltz56piei66drc63vkh5yixiyk4cme rrjtid.onion/
XSS forum	http://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/
TruthBoard	http://k5aintllrufq23khjnmfli6uxioboe3ylcao7k72mk2bgvwqb5ek4ad.onion/
Best Carding World	http://bestteerm42clir6ux7xm76d4jjodh3fpahjqgdbdbmfrgp4skg2wqd.onion/
Cebulga Polish forum	http://cebulka7uxchnbpvmqapg5pfos4ngaxglsktzvha7a5rigndghvadeyd.onion/
DeepLink	http://deeeepv4bfndyatwkdzeciebcqwwlvqga6mofdtvswpon4e1fut7lfqd.onion/Cat/4/Page/2
Reverse4you	https://forum.reverse4you.org/
Sabote	https://sabote.org/
Greekhacking	https://greekhacking.gr/

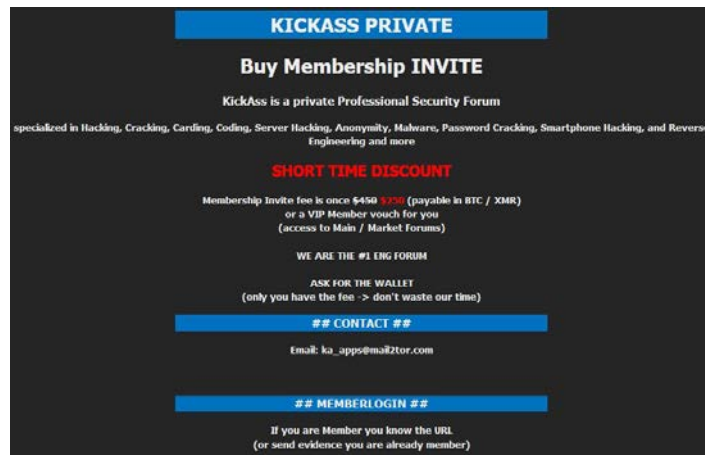
Στα περισσότερα φόρουμ υπάρχουν συζητήσεις για θέματα κρυπτογραφίας, ιούς και malware, δικτύων, προγραμματισμού και φυσικά πιθανών ευπαθειών σε πληροφοριακά συστήματα. Τα τελευταία χρόνια υπάρχουν συζητήσεις για εφαρμογές κινητών τηλεφώνων, κυρίως με λειτουργικό Android.

Η πρόσβαση σε ένα τέτοιο φόρουμ μπορεί να είναι δωρεάν, μπορεί όμως να απαιτείται και κάποια πληρωμή ώστε να αποθαρρύνονται να συμμετέχουν απλοί χρήστες χωρίς εμπειρία ή κάποια μέλη των διωκτικών αρχών.



TOPICS	POSTS	LAST POST
Penetration Tests Penetration testing	25	39
Social Engineering Tests Social Engineering Testing	19	25
Exploits Exploiting	16	23
Tools Tools	93	127
Malware Viruses & Malware	29	41
Cryptography Cryptography	8	12
Others Programming, Wireless, mobiles and other hardware, Physical security, Tutorials and more	112	140
Hacking Tutorials Free Hacking Tutorials	156	194
Hacked Accounts and Database Dumps Share the Goods with Best Carding World Members	1245	1625
Android Modded apk Hacked and Modified Android Applications	312	316

Εικόνα Β' 0.3: Screenshot από το Best Carding World forum



Εικόνα Β'.0.4 Αγορά συνδρομής στο KickAss forum

B.2 Αγορά κακόβουλου λογισμικού

Το κακόβουλο ή ιομορφικό λογισμικό εξελίσσεται παράλληλα με τις νόμιμες αγορές προϊόντων λογισμικού, αφού προσπαθεί να εκμεταλλευτεί την εξέλιξη που υπάρχει σε αυτές, ώστε να αποκτήσει πρόσβαση σε προσωπικούς υπολογιστές, κινητά τηλέφωνα, tablets ή και εξυπηρετητές εταιριών.

Η πιο σημαντική ίσως αγορά εδώ είναι το *λογισμικό λύτρων* (ransomware), δηλαδή λογισμικό το οποίο επιτρέπει σε κάποιον κακόβουλο χρήστη να αποκτήσει πρόσβαση σε προσωπικά ή εταιρικά δεδομένα με σκοπό τον εκβιασμό και την απόκτηση λύτρων.

Στο dark web το μοντέλο Ransomware-as-a-service (RaaS) είναι το κυρίαρχο μοντέλο διανομής τέτοιου λογισμικού, επιτρέποντας έτσι σε ανθρώπους που δεν έχουν μεγάλη πείρα σε προγραμματισμό να γίνουν οι ίδιοι επιτιθέμενοι ή να συμμετάσχουν ως μέλη μιας μεγαλύτερης ομάδας σε επιθέσεις λύτρων. Με τον τρόπο αυτό καθημερινοί άνθρωποι γίνονται συνένοχοι σε εγκληματικές ενέργειες ενώ μειώνεται και ο κίνδυνος σύλληψης για τους πιο έμπειρους χρήστες.

Για παράδειγμα κάποιος δυσαρεστημένος υπάλληλος μιας εταιρίας, μπορεί να συνεργαστεί με έναν ή περισσότερους προγραμματιστές RaaS λογισμικού για να χτυπήσουν την εταιρία εκ των έσω και έπειτα να μοιραστούν τα κέρδη. [2]

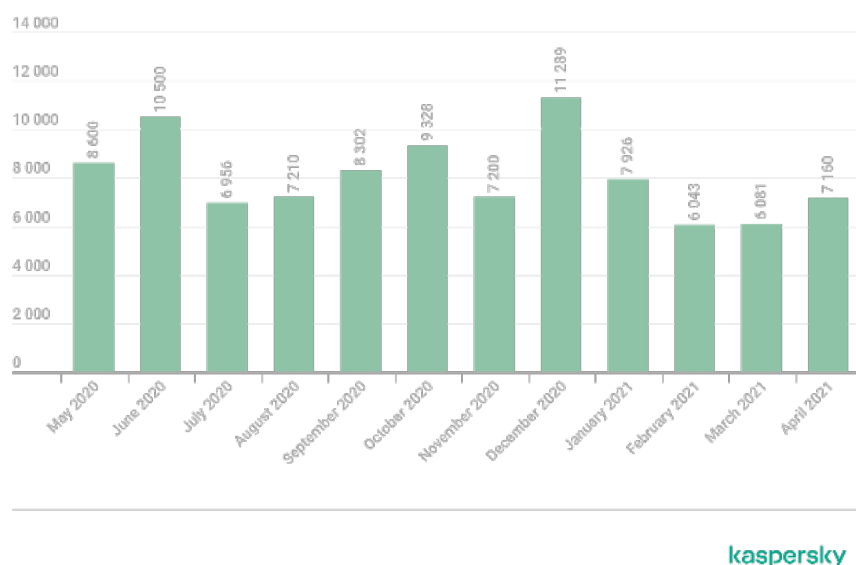
Σύμφωνα με τον Peter Gutmann του Πανεπιστημίου του Auckland, στο dark web το malware γενικότερα πωλείται (και διαφημίζεται) ως Malware as a Service (MaaS), όπως ακριβώς οι κατασκευαστές νόμιμου λογισμικού έχουν υιοθετήσει το μοντέλο Software as a Service (SaaS).

Το μοντέλο SaaS, το οποίο στην δική μας περίπτωση υλοποιείται ως MaaS, παρέχει λογισμικό. Προσφέρει δηλαδή στον αγοραστή τη δυνατότητα να κάνει χρήση εφαρμογών

που προσφέρει ο πωλητής. Οι εφαρμογές αυτές είναι προσβάσιμες με τη χρήση κάποιου browser ή μέσω τοπικά εγκατεστημένου λογισμικού. Ο χρήστης δεν έχει την δυνατότητα διαχείρισης και ελέγχου των υποδομών, δηλαδή των εξυπηρετητών του δικτύου, των λειτουργικών συστημάτων, του αποθηκευτικού χώρου, ακόμη και μερικών δυνατοτήτων των εφαρμογών. Μπορεί όμως να παραμετροποιήσει την εφαρμογή και να την χρησιμοποιήσει για δικό του όφελος. Το μοντέλο αυτό αντιπαρατίθεται με άλλες δύο μορφές παροχής λογισμικού, που έχουν αυξημένες δυνατότητες για τον χρήστη, το IaaS και το PaaS.

Το μοντέλο Platform-as-a-Service (PaaS) παρέχει την πλατφόρμα στην οποία ο χρήστης έχει τη δυνατότητα να δημιουργήσει ή να εγκαταστήσει αν θέλει το δικό του πακέτο εφαρμογών επάνω στις υποδομές του παρόχου. Επίσης, περιέχει εργαλεία για την κατασκευή ή την διαχείριση των εφαρμογών (γλώσσες προγραμματισμού, βιβλιοθήκες, υπηρεσίες, εργαλεία ανάπτυξης). Ο χρήστης δεν διαχειρίζεται και δεν έχει τον έλεγχο των υποδομών που βασίζονται στο PaaS, αλλά έχει τον έλεγχο των εφαρμογών του και πιθανώς κάποιων ρυθμίσεων του περιβάλλοντος που φιλοξενεί τις εφαρμογές.

Το μοντέλο Infrastructure-as-a-Service (IaaS) παρέχει φυσικές υποδομές προσφέροντας στο χρήστη τη δυνατότητα ελέγχου της υπολογιστικής ισχύος, αποθηκευτικού χώρου, ταχύτητας και φόρτου δικτύου και άλλων πληροφοριακών πόρων. Αφορά στην παροχή υπολογιστικών πόρων, ώστε ο χρήστης να μην χρειάζεται να αγοράσει εξυπηρετητές, λογισμικό ή δικτυακό εξοπλισμό και σύνδεση. Σε όλα αυτά μπορεί επίσης να περιέχονται λειτουργικά συστήματα και εφαρμογές. Δεν υπάρχει η δυνατότητα διαχείρισης των προσφερόμενων υποδομών από το χρήστη.



Εικόνα Β' 0.5 Πλήθος επιθέσεων ανά μήνα στην Ευρώπη

Σύμφωνα με την εταιρία Kaspersky μια ακόμα πολύ σημαντική απειλή για τους τελικούς χρήστες αφορά το τραπεζικό τους απόρρητο. Οι προσπάθειες κλοπής χρημάτων από τους τραπεζικούς λογαριασμούς χρηστών, μέσω κακόβουλου λογισμικού στον υπολογιστή τους, ανέρχονται σε αρκετές χιλιάδες μηνιαίως, στις χώρες της Ευρωπαϊκής Ένωσης.

Στο παραπάνω διάγραμμα φαίνονται οι αριθμοί των επιθέσεων που έχουν αποτραπεί μέσα σε έναν χρόνο, από τον Μάιο 2020 ως τον Απρίλιο 2021, μόνο σε Ευρωπαϊκές χώρες.

Στο ίδιο χρονικό διάστημα, οι κυριότερες απειλές που εμφανίστηκαν σε αυτές τις επιθέσεις είναι :

Πίνακας Β' 0.4 Οι δέκα πιο συχνές απειλές στην Ευρώπη

	<u>Όνομα</u>	<u>Ποσοστό %</u>
1	Zbot	24.7
2	Nymaim	11.5
3	Danabot	9.9
4	Emotet	8.9
5	CliptoShuffler	7.7
6	BitStealer	5.6
7	SpyEyes	3.5
8	Gozi	3.4
9	Dridex	3.2
10	Trickster	1.9

Αντίστοιχα μεγάλος με τα ποσοστά που φαίνονται στον πίνακα, είναι ο αριθμός των χρηστών που δέχθηκαν επίθεση από ransomware Trojans. [11]

Πολλαπλάσιος όμως (διπλάσιος ή και τριπλάσιος ανά μήνα) είναι ο αριθμός των επιθέσεων μέσω miners, δηλαδή προγραμμάτων εξόρυξης κρυπτονομισμάτων. Η προσπάθεια όλο και περισσότερων χρηστών υπολογιστικών συστημάτων να συμμετάσχουν στην εξόρυξη κρυπτονομισμάτων, γίνεται στόχος κακόβουλων χρηστών, οι οποίοι προσπαθούν να εγκαταστήσουν Trojans στους υπολογιστές τους (όπως τον Trojan.Win32.Miner.gen)

Σύμφωνα με τον ανεξάρτητο οργανισμό AVtest, τα τελευταία δέκα χρόνια, το κακόβουλο λογισμικό που κυκλοφορεί σε όλων των ειδών τις συσκευές και λειτουργικά συστήματα, αυξήθηκε από τα 100 εκατομμύρια περίπου, στα 1289 εκατομμύρια. [12]

Ωστόσο οι αριθμοί αυτοί είναι μόνο εκτιμήσεις, καθώς βασίζονται σε δεδομένα εταιριών κυβερνο-ασφάλειας από επιθέσεις που έχουν αποτραπεί σε συγκεκριμένες μάλιστα γεωγραφικές αγορές. Οι επιθέσεις όμως που υπήρξαν επιτυχημένες πολλές φορές δεν αναφέρονται από τα θύματα, για διάφορους λόγους, και επομένως δεν καταγράφονται.

B.3 Μελέτες για το πλήθος των συναλλαγών στο dark web

Υπάρχει ένα εγγενές πρόβλημα συλλογής δεδομένων για τις δραστηριότητες στο Dark Web. Πολλές μελέτες έχουν γίνει μέχρι σήμερα, από ανεξάρτητους οργανισμούς και Πανεπιστήμια, για το είδος και το πλήθος των δραστηριοτήτων των ιστοσελίδων του. Οι υπεύθυνοι του Tor browser εκτιμούν ότι μόνο το 1,5% των χρηστών του επισκέπτονται παράνομες ιστοσελίδες στο Dark Web. Ωστόσο, αφού ο ακριβής αριθμός ιστοσελίδων που εξυπηρετούν αγορά παράνομων προϊόντων και υπηρεσιών είναι ακαθόριστος, είναι δύσκολο να προσδιοριστεί και το πλήθος των χρηστών που κατευθύνονται εκεί. [13]

Σημαντικό επίσης πρόβλημα αποτελεί η ύπαρξη σελίδων και forum σε διαφορετική γλώσσα από την Αγγλική. Η Ρωσική όπως και η Αραβική γλώσσα εμφανίζονται αρκετά συχνά.

- Μελέτη του Πανεπιστημίου του Πόρτσμουθ εξέτασε την κίνηση των χρηστών του TOR προς τέτοιες κρυφές υπηρεσίες. Οι ερευνητές έστησαν 40 ενδιάμεσους κόμβους του δικτύου Tor με σκοπό να ανιχνεύσουν το πλήθος των κρυφών σελίδων – περίπου 45.000 – και να μελετήσουν την κίνηση προς αυτές. Σύμφωνα με την μελέτη, το συντριπτικό ποσοστό των επισκέψεων αφορούσαν σελίδες παιδικής πορνογραφίας.
- Μια άλλη μελέτη από το King's College του Λονδίνου αφορούσε επίσης το ίδιο θέμα, τον αριθμό των κρυφών υπηρεσιών στο Dark Web. Ξεκινώντας από δύο δημοφιλείς μηχανές αναζήτησης, τις Ahmia και OnionCity, χρησιμοποίησαν web crawlers για να αναγνωρίσουν 5.205 ενεργές σελίδες. Από αυτές μπόρεσαν να ελέγξουν το περιεχόμενο σε 2.723 σελίδες. Οι 1547 περιείχαν παράνομο περιεχόμενο. Η εικόνα αυτή είναι απλά ενδεικτική των ποσοστών των σελίδων που προσπελάζονται μέσω Tor. Το 2015, η εκτίμηση ήταν ότι περίπου 30.000 σελίδες με παράνομο περιεχόμενο ήταν ενεργές καθημερινά. Νεότερα στοιχεία του 2017 ανέβαζαν τον αριθμό αυτό σε περίπου 60.000 καθημερινά. [13]

Τι ακριβώς πωλείται σε αυτές τις σελίδες; Πολλά και διαφορετικά προϊόντα – υπηρεσίες.

- Υπάρχουν fora με συζητήσεις για θέματα φοροδιαφυγής και οικονομικών απαλλαγών
- Malware για υποκλοπή στοιχείων πιστωτικών – χρεωστικών καρτών από ηλεκτρονικούς υπολογιστές κατά την διάρκεια ηλεκτρονικών αγορών.
- Ram scrapers που εγκαθίστανται σε τερματικές συσκευές (POS) και υποκλέπτουν στοιχεία των καρτών που εισάγονται σε αυτές, όπως έγινε το 2013 με την παραβίαση της εταιρίας ηλεκτρονικών πληρωμών Target. Κλάπηκαν πάνω από 40 εκατομμύρια αριθμοί πιστωτικών ή χρεωστικών καρτών και περίπου 70 εκατομμύρια διευθύνσεις, τηλέφωνα και άλλα προσωπικά δεδομένα. [14] Για εβδομάδες μετά την επίθεση, οι

αριθμοί πιστωτικών καρτών πωλούνταν στην μαύρη αγορά του Dark Web, προς 20\$ ως 100\$ ο καθένας.

- Ransomware δηλαδή λογισμικό που κρυπτογραφεί τα δεδομένα του χρήστη στον υπολογιστή που θα εγκατασταθεί και αναρτά ένα μήνυμα για πληρωμή λύτρων, ώστε να λάβει ο χρήστης το κλειδί αποκρυπτογράφησης και να σώσει τα δεδομένα του.
- Leaked databases δηλαδή ολόκληρες βάσεις δεδομένων εταιριών ή οργανισμών που έχουν υποκλαπεί. Σε κάποιες περιπτώσεις μπορεί να είναι αποσπάσματα μιας βάσης δεδομένων, που όμως μπορεί να ενδιαφέρουν κάποιους αγοραστές, όπως οικονομικά στοιχεία μιας εταιρίας ή ένα πλήθος από εταιρικά emails.
- Botnets – Loaders δηλαδή προγράμματα που μπορούν να λειτουργήσουν ως Δούρειοι Ίπποι όταν εγκατασταθούν σε κάποιο υπολογιστικό σύστημα και να επιτρέψουν σε κακόβουλους χρήστες να αποκτήσουν πρόσβαση σε αρχεία, κωδικούς ή να φορτώσουν άλλα προγράμματα όπως ransomware.
- Exploit kits δηλαδή προγράμματα που εκμεταλλεύονται μια ευπάθεια που έχει διαπιστωθεί στο λειτουργικό σύστημα μιας συσκευής, ώστε να αποκτήσουν πρόσβαση σε εταιρικά δίκτυα ή υπολογιστές.

B.4 Εξέλιξη κόστους

Το κόστος των προϊόντων στο Dark web ποικίλει, με βάση την ποιότητα του προϊόντος, τη φήμη του πωλητή και τις εξειδικευμένες απαιτήσεις του αγοραστή, την ημερομηνία πρώτης κυκλοφορίας του κ.α.

Η ποιότητα μπορεί να οριστεί με όρους ευκολίας χρήσης και ολοκληρωμένης λειτουργίας. Υπάρχουν διαρροές δεδομένων που αφορούν μόνο ένα κομμάτι μιας επιχείρησης, για παράδειγμα μόνο ένα τμήμα της παραγωγής ή ένα ορισμένο πελατολόγιο, επομένως κοστίζουν λιγότερο από μια ολοκληρωμένη βάση.

Σε προϊόντα λογισμικού, ένα πρόγραμμα ransomware-as-a-service το οποίο μπορεί να χρησιμοποιηθεί άμεσα και με ευκολία από τον αγοραστή, θα κοστίζει περισσότερο από κάποιο άλλο που θα χρειαστεί compilation και παραμετροποίηση.

Όταν ένα προϊόν είναι καινούριο ή εκμεταλλεύεται μια άγνωστη ακόμα ευπάθεια η τιμή του είναι υψηλή, όσο όμως περνάει ο καιρός και εμφανίζονται ενημερώσεις ασφαλείας τις οποίες εφαρμόζουν οι χρήστες υπολογιστικών συστημάτων, τόσο πέφτει η τιμή του, αφού το ίδιο προϊόν είναι πλέον αναποτελεσματικό.

Exploit kits πωλούνται σε τιμές από 15\$ ως 10.000\$ ενώ το κόστος υπηρεσιών εξαρτάται από την διάρκεια. Το 2011 το Blackhole 1.2.1 κόστιζε 700\$ για 3 μήνες και 1500\$ για έναν

χρόνο. Το Roborack κόστιζε 150\$ την εβδομάδα και 500\$ τον μήνα περίπου. Τα zero-day exploits πετυχαίνουν πολύ καλύτερες τιμές.

Το 2012 η εκτίμηση τιμών για τέτοια προϊόντα ήταν 60.000\$ ως 120.000\$ για τα Windows, 150.000\$ ως 250.000\$ για το iOS, 30.000\$ ως 60.000\$ για το Android και 5.000\$ ως 30.000\$ για τον Acrobat reader. [15]

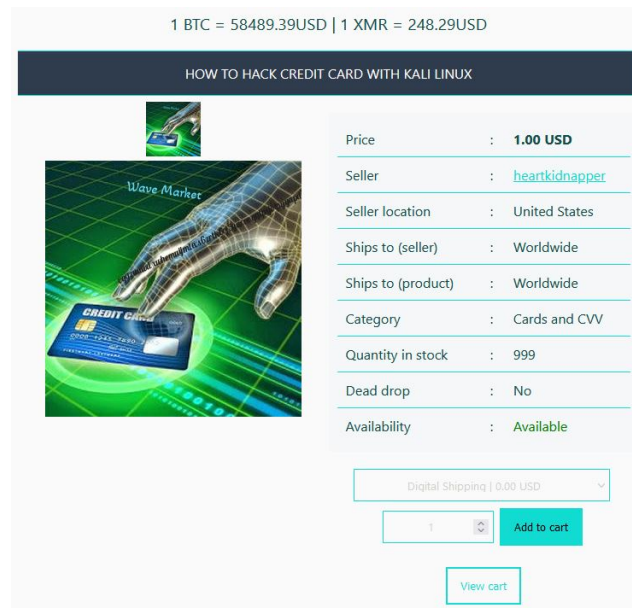
Βάσεις δεδομένων που έχουν διαρρεύσει μπορούν άμεσα να πιάσουν το ποσό των 1500\$, ενώ εξακολουθούν να πωλούνται ακόμα και για 7-8 χρόνια μετά την πρώτη διαρροή τους, όμως οι τιμές τους είναι πολύ μικρές, της τάξης των 40\$ – 50\$.

B.5 Σημεία πώλησης

Τα σημεία πώλησης είναι πολλά, όμως δεν διαθέτουν όλα την ίδια αξιοπιστία ούτε απευθύνονται στο ίδιο κοινό. Υπάρχουν σελίδες που έχουν γραφικό περιβάλλον και απευθύνονται στον άπειρο αγοραστή, ο οποίος κάνει μια επιφανειακή αναζήτηση στο dark web.

Τέτοιοι χρήστες περιμένουν να συναντήσουν ένα γνώριμο περιβάλλον, παρόμοιο με αυτό των νόμιμων ιστοσελίδων, στο οποίο θα μπορούν να περιηγηθούν εύκολα. Έτσι βρίσκουμε συχνά αναρτήσεις του τύπου :

- «Iframe exploits, pop-unders, click fraud, posting, spam If you don't have it, you can rent it here. Online video tutorials of the malware in action»
- «Traffic for spoils Free trial, 100 visitors!!!
Price
 - o \$4 per 1000 if buying 1000 – 5000
 - o \$3.80 per 1000 if buying 5000 – 10,000
 - o \$3.50 per 1000 if buying over 10,000»
- «Buy the basic version for \$1000-2000 (Gozi). Purchase add-on services at varying prices starting at \$20»
- «How to hack credit card with Kali Linux»
- Χρήση iframe, διαφημίσεων pop-under, απάτη κλικ, spam μηνύματα: αν δεν τα έχετε ήδη, νοικιάστε τα εδώ. Δείτε βίντεο online με το κακόβουλο λογισμικό σε δράση.
- Ψεύτικες επισκέψεις σε αναρτήσεις σας. Δωρεάν δοκιμή 100 επισκέψεις!!!
Τιμές:
 - o 4\$ ανά 1000, αγοράζοντας 1000-5000
 - o 3.80\$ ανά 1000, αγοράζοντας 5000-10000
 - o 3.50\$ ανά 1000, αγοράζοντας 10000 και άνω
- Αγοράστε την βασική έκδοση για 1000-2000\$. Αγοράστε επιπλέον υπηρεσίες με τιμές από 20\$
- Πώς να χακάρετε πιστωτική κάρτα με το Kali Linux



Εικόνα Β' 0.6 GUI ηλεκτρονικού καταστήματος στο Dark web

Στις σελίδες αυτές υπάρχει καλάθι αγορών, στο οποίο ο αγοραστής τοποθετεί τα προϊόντα που θα αγοράσει. Η εικόνα που δίνεται είναι παρόμοια με αυτή των νόμιμων eshops, με τα οποία ο απλός χρήστης είναι εξοικειωμένος. Όμως η υπερβολική ευκολία προιδεάζει για πιθανή απάτη.

Τρία είναι τα σημεία που θα πρέπει να προβληματίσουν τον αγοραστή λογισμικού ransomware. Πρώτα η αξιολόγηση του πωλητή να προέρχεται κυρίως από την πώληση άλλων παράνομων ειδών, όπως ναρκωτικά ή πιστωτικές κάρτες. Δεύτερο είναι η περιγραφή των προϊόντων λογισμικού να είναι ασαφής και τυποποιημένη, ενώ η τιμή του είναι πολύ χαμηλή. Τρίτο να μην υπάρχουν εξηγήσεις για τις θετικές αξιολογήσεις, γεγονός που υποδεικνύει αυτόματη δημιουργία τους, ενώ οι αρνητικές αξιολογήσεις να είναι περισσότερο τεκμηριωμένες.

Σε κάποιες περιπτώσεις αναφέρονται εξηγήσεις για κάποια αρνητική αξιολόγηση, όπως ότι «τα αρχεία αυτά είναι αρχεία ανοιχτού κώδικα που βρίσκει κανείς δωρεάν στο Github και είναι παλιά». [2]

<u>Ransomware for 55\$ / Features :</u> Uses AES algorithm to encrypt files. Sends encryption key to a server. Encrypted files can be decrypt in decrypter program with encryption key. Creates a text file in Desktop with given message. Small file size (12 KB) NOT detected by antivirus programs»	<u>Ransomware για 55\$ / Χαρακτηριστικά:</u> Χρησιμοποιεί αλγόριθμο AES για κρυπτογράφηση των αρχείων Στέλνει το encryption key σε έναν server. Τα κρυπτογραφημένα αρχεία μπορούν να αποκρυπτογραφηθούν με χρήση του κατάλληλου κλειδιού. Δημιουργεί ένα αρχείο κειμένου στην επιφάνεια εργασίας με συγκεκριμένο μήνυμα. Μικρό μέγεθος αρχείου (12KB) ΔΕΝ ανιχνεύεται από προγράμματα antivirus.
--	---

Price	: 55.00 USD
Seller	: drhack3r
Seller location	: Worldwide
Ships to (seller)	: Worldwide
Ships to (product)	: Worldwide
Category	: Hacks
Quantity in stock	: 999
Dead drop	: No
Availability	: Available

Εικόνα Β' 0.7 Πώληση ransomware από πιθανώς αναξιόπιστο πωλητή

Σε πολλές περιπτώσεις υπάρχει εξειδικευμένο GUI, απολύτως φιλικό προς τον χρήστη. Κάποιες σελίδες όμως απαιτούν σύνδεση με username/password, γεγονός βέβαια που καταργεί την ανώνυμη πρόσβαση του χρήστη.

1 BTC = 58518.59USD | 1 XMR = 248.28USD

Please login to use our services.

Username

Password

1 hour

YRUHAY

Captcha

Login

Create account Recover account

Εικόνα Β' 0.8 Logon screen σε κάποια σελίδα του Dark web

Συνήθως τα προϊόντα συνοδεύονται από σχόλια που περιγράφουν τα χαρακτηριστικά τους και διαφημίζουν τον πωλητή. Η πείρα και η αξιοπιστία του πωλητή φαίνεται ότι παίζουν σημαντικό ρόλο και στο συγκεκριμένο χώρο πωλήσεων, αφού αυξάνουν τις τιμές αλλά και την πελατεία του. Πολλοί είναι αυτοί που καταφεύγουν σε επιθετικό μάρκετινγκ για να διασφαλίσουν το όνομά τους και να πουλήσουν το προϊόν. Όπως το παρακάτω, που συνοδεύεται από τα εξής:

Πίνακας Β 0.5 Επιθετικό μάρκετινγκ από hacker

WELCOME! ***** I've been in the fraud business for many years, even before internet fraud was a thing. I started working with fake checks cloned cards, but then moved completely to digital fraud once I discovered it (mid 2011-12).	ΚΑΛΩΣΗΛΘΑΤΕ Βρίσκομαι στο χώρο των εξαπατήσεων για πολλά χρόνια, πριν ακόμα υπάρχουν οι διαδικτυακές απάτες. Ξεκίνησα με ψεύτικες επιταγές, ψεύτικες κάρτες αλλά πέρασα στις δικτυακές απάτες, αμέσως μόλις τις
---	---

It took me a long time and a lot of trial and error to know what I know now. The fraud business is an ever-changing type of business, meaning methods are constantly being updated because of new security implementations on the market. For many years, I worked by myself, lived the good life, and did not share any methods. Around mid 2015, I became a vendor on Alphabay Market, and quickly became one of the top names in the fraud business. A success that has only grown more and more with time. With this success, I decided to teach others what I do, to not only add value to peoples lives, but also to meet new connections and make a group of like-minded individuals, which in my opinion is one of the secrets to success. ***** SERVICE ***** LUXSOCKS is currently the best SOCKS5 provider in the market. The regular price on their website for an account is \$500. I sell for half that price. MY ACCOUNTS ARE HACKED, BUT THEY LAST FOREVER AS LONG AS YOU CHANGE PASSWORD, RECOVERY EMAIL JABBER! I AM NOT RESPONSIBLE FOR BUYERS THAT DO NOT CHANGE ACCOUNT DETAILS, AND LOSE ACCESS BECAUSE ORIGINAL OWNER CHANGED PASSWORD! I will do everything in my power to make sure you are 100% satisfied with your order. If for any reason you are not satisfied, PLEASE CONTACT ME FIRST BEFORE LEAVING NEGATIVE FEEDBACK OR DISPUTING THE TRANSACTION! DISPUTES LEAVE A PERMANENT STAIN ON MY PROFILE THAT I CANNOT REMOVE. BUYERS THAT OPEN DISPUTES WITHOUT CONTACTING WILL BE BLOCKED FROM FUTURE PURCHASES! ***!!(IMPORTANT)!** THERE ARE MANY IMPOSTERS/FAKES TRYING TO MAKE MONEY OFF MY NAME, BE CAREFUL AND ALWAYS ASK FOR PGP SIGNED MESSAGE TO VERIFY IDENTITY!	ανακάλυψα (2011-12). Χρειάστηκα πολύ χρόνο, κόπο και αποτυχημένες προσπάθειες για να μάθω. Η εξαπάτηση είναι μια διαρκώς εξελισσόμενη επιχείρηση, αφού οι μέθοδοι και οι προδιαγραφές ασφαλείας στην αγορά, αλλάζουν διαρκώς. Για πολλά χρόνια εργάστηκα μόνος μου, ώστε να μην μοιράζομαι τις μεθόδους μου. Από το 2015 έγινα μέλος του Alphabay Market, και γρήγορα έγινα ένα από τα μεγαλύτερα ονόματα στον χώρο. Με τέτοια επιτυχία αποφάσισα να διδάξω και άλλους την μέθοδό μου, ώστε να τους βοηθήσω να βελτιώσουν τη ζωή τους και να φτιάξω την δική μου ομάδα. Η LUXSOCKS είναι σήμερα η καλύτερη υπηρεσία παροχής SOCKS5 στην αγορά. Η τιμή τους για ένα λογαριασμό είναι 500\$, εγώ όμως πουλάω στην μισή τιμή. Οι λογαριασμοί μου είναι «χακαρισμένοι», όμως διαρκούν για πάντα αν αλλάξετε κωδικό και email επαναφοράς. Δεν φέρω ευθύνη για πελάτες που έχασαν τον λογαριασμό τους επειδή δεν άλλαξαν τα στοιχεία εγκαίρως. Θα κάνω ότι είναι δυνατόν για να μείνετε 100% ικανοποιημένοι με την παραγγελία σας. Αν για οποιονδήποτε λόγο δεν είστε ικανοποιημένοι, ΠΑΡΑΚΑΛΩ ΕΠΙΚΟΙΝΩΝΗΣΤΕ ΜΑΖΙ ΜΟΥ ΠΡΙΝ ΔΩΣΕΤΕ ΑΡΝΗΤΙΚΗ ΑΞΙΟΛΟΓΗΣΗ Η ΑΚΥΡΩΣΕΤΕ ΤΗΝ ΠΑΡΑΓΓΕΛΙΑ. Οι ακυρώσεις είναι μια μόνιμη κηλίδα στο προφίλ μου, την οποία δεν μπορώ να διαγράψω. Όσοι πελάτες κάνουν ακυρώσεις χωρίς να με ενημερώσουν θα μπλοκάρονται μόνιμα από μελλοντικές παραγγελίες. ΣΗΜΑΝΤΙΚΟ : Υπάρχουν πολλοί μιμητές που προσπαθούν να βγάλουν χρήματα χρησιμοποιώντας το όνομά μου, να είστε προσεκτικοί και να ζητάτε πάντα ένα PGP κρυπτογραφημένο μήνυμα για να επιβεβαιώσετε την ταυτότητά μου.
---	--

Οι τιμές παρέχονται σε USD αλλά ταυτόχρονα δίνεται η ισοτιμία BTC-USD (bitcoin), XMR-USD (monero), που είναι τα δύο αποδεκτά ψηφιακά νομίσματα με τα οποία θα γίνει η πληρωμή στον συγκεκριμένο πωλητή.

1 BTC = 58678.4USD | 1 XMR = 246.58USD

BUNDLE HACKING TOOLS TO BECOME A MILLIONAIRE



Price	:	312.01 USD
Seller	:	g3cko
Seller location	:	Worldwide
Ships to (seller)	:	Worldwide
Ships to (product)	:	Worldwide
Category	:	Hacks
Quantity in stock	:	100000
Dead drop	:	No
Availability	:	Available

Εικόνα Β 0.9 Πώληση hacking tools

Private and fud clipper stealer btc compiled for 89\$ «Replacing a wallet with a wallet similar to that from your list in the file Defines the first and last wallet characters»	Υποκλοπή bitcoins από προσωπικό ή εταιρικό πορτοφόλι για 89\$ Αντικαθιστά ένα πορτοφόλι με ένα άλλο παρόμοιο, αλλάζει τον πρώτο και τον τελευταίο χαρακτήρα
--	---

1 BTC = 58642.29USD | 1 XMR = 247.01USD

PRIVATE AND FUD CLIPPER STEALER BTC COMPILED



Price	:	89.00 USD
Seller	:	eternos
Seller location	:	Worldwide
Ships to (seller)	:	Worldwide
Ships to (product)	:	Worldwide
Category	:	Hacks
Quantity in stock	:	19
Dead drop	:	No
Availability	:	Available

Εικόνα Β 0.10 Πώληση Bitcoin stealer

B.6 Η συνολική εικόνα σήμερα

Ποιο είναι όμως το συγκεντρωτικό κόστος της παράνομης αγοράς λογισμικού στο dark web; Θα μπορούσε κάποιος φορέας να το υπολογίσει και εάν ναι, σε ποια χρονική βάση και με ποια κριτήρια;

Μια λογική υπόθεση είναι να προσπαθήσουμε να υπολογίσουμε το ετήσιο κόστος της χρήσης παράνομου λογισμικού, που διακινήθηκε μέσω του dark web.

Η διακίνηση του λογισμικού έχει βέβαια δύο κόστη. Το πρώτο είναι το κόστος απόκτησης, δηλαδή τα χρήματα που θα πληρώσει κάποιος στον πωλητή, για να αποκτήσει ιομορφικό λογισμικό, κλεμμένους λογαριασμούς, κ.α. (άμεσο κόστος). Το δεύτερο είναι το κόστος από την χρήση, δηλαδή η ζημιά που θα επιφέρει στην αγορά, όπως το ποσό που θα καταφέρει

κάποιος να χρεώσει σε κλεμμένους τραπεζικούς λογαριασμούς ή πιστωτικές κάρτες, τα λύτρα για ransomware, η καταστροφή δεδομένων, οι χαμένες εργατοώρες κ.α. (έμμεσο κόστος). Θα μπορούσαμε να συνυπολογίσουμε στα παραπάνω και ένα ακόμη κόστος, αυτό που ξοδεύεται από εταιρίες αλλά και ιδιώτες για την προστασία από το κακόβουλο λογισμικό. (αμυντικό κόστος ή κόστος πρόληψης).

Με μια πρώτη ματιά, φαίνεται ότι το άμεσο κόστος είναι πολύ μικρό, ενώ το έμμεσο θα είναι πολύ μεγαλύτερο αν συνυπολογίσει κανείς τα ποσά των αποζημιώσεων που μπορεί να δίνονται. Το μεγαλύτερο όλων όμως είναι το κόστος άμυνας, μια βιομηχανία στην οποία οι εταιρίες ξοδεύουν ετησίως εκατομμύρια δολάρια. Ένα χαρακτηριστικό παράδειγμα προέρχεται από στοιχεία του 2010. Το έτος αυτό, ένα botnet που θεωρήθηκε υπεύθυνο για το 1/3 του συνολικού spam messaging παγκοσμίως, φαίνεται να απέφερε στους δημιουργούς του μόλις 2.7 εκατομμύρια δολάρια, ενώ προφανώς το ετήσιο κόστος πρόληψης του spam παγκοσμίως είναι πολύ μεγαλύτερο.

Το παγκόσμιο κόστος για το έτος 2021 υπολογίζεται στα 6 τρισεκατομμύρια δολάρια με μια ανοδική τάση περίπου 15% ανά έτος. Εάν η άνοδος συνεχιστεί με τον ίδιο ρυθμό, το κόστος θα ξεπεράσει τα 10 τρις δολάρια το έτος 2025. [16]

Σύμφωνα με κάποιες αναφορές το κυβερνο-έγκλημα μπορεί να κοστίζει πολύ ακριβά κυρίως στις ανεπτυγμένες περιοχές του πλανήτη. Το 0.41% του ΑΕΠ στην Ευρώπη και το 0.61% στις ΗΠΑ, ενώ σε συγκεκριμένες περιπτώσεις χωρών μπορεί να είναι πολύ μεγαλύτερο, όπως το 1.60% του ΑΕΠ στην Γερμανία. [17]

Ωστόσο το ερώτημα σχετικά με τον τρόπο υπολογισμού παραμένει. Σύμφωνα με την παραπάνω μελέτη, πολλοί ακαδημαϊκοί αμφισβητούν τα ποσά και τα θεωρούν υπερβολικά. Θεωρούν επίσης ότι η συστηματική ποσοτική μελέτη του κόστους είναι πολύ περιορισμένη και βασίζεται κυρίως σε ερωτηματολόγια και εμπειρικά στοιχεία.

B.7 Η ετήσια εξέλιξη της αγοράς τα τελευταία χρόνια

Η ταχεία μεταφορά πολλών πτυχών της καθημερινής ζωής αλλά και της επιχειρηματικής δραστηριότητας την τελευταία δεκαετία, από τον πραγματικό στον ψηφιακό κόσμο, έφερε αντίστοιχη αύξηση του κόστους του κυβερνο-εγκλήματος. Για τους πολίτες το κινητό τηλέφωνο αντικατέστησε τον Ηλεκτρονικό Υπολογιστή, το Android αντικατέστησε τα Windows ενώ για τις εταιρίες πολλές ενδο-εταιρικές υπηρεσίες μετατράπηκαν σε υπηρεσίες νέφους.

Η χρήση των κοινωνικών δικτύων την ίδια περίοδο γνώρισε ταχεία εξάπλωση. Το αποτέλεσμα αυτής της εξέλιξης είναι σήμερα, το μισό περίπου έγκλημα σε πλήθος και αξία

να βρίσκεται online. Ορισμένες αλλαγές είναι ενδιαφέρουσες, όπως ότι οι απάτες ηλεκτρονικών πληρωμών έχουν διπλασιαστεί σε χρηματική αξία όμως έχουν μειωθεί ποσοστιαία σε σχέση με το συνολικό ποσό online πληρωμών. Αυτό οφείλεται στο γεγονός ότι οι ηλεκτρονικές πληρωμές έχουν πολλαπλασιαστεί και έχουν θωρακιστεί αρκετά. [18]

Πολλές νέες μορφές κυβερνο-απάτης έχουν αυξηθεί τόσο ώστε να έχουν αξιοσημείωτη αξία, όπως η κλοπή εταιρικών email και το cryptojacking. Επίσης κάποιες παραδοσιακές σχετικές με φορολογία και τεκμήρια έχουν μεταφερθεί πλέον online, ώστε να θεωρούνται κυβερνο-απάτες, ενώ εξακολουθούν να κοστίζουν σε κάθε φορολογούμενο πολίτη εκατοντάδες δολάρια ή ευρώ.

Το ερώτημα σχετικά με το συνολικό κόστος παραμένει, καθώς θα έδινε και μια απάντηση στα ποσά που είναι συμφέρον να δαπανήσουν οι κυβερνήσεις για την πρόληψη και αντιμετώπιση του κυβερνο-εγκλήματος, ωστόσο είναι δύσκολο να απαντηθεί συνολικά. Ένα ακόμη χαρακτηριστικό παράδειγμα είναι ότι ένα botnet του 2011 το οποίο απέφερε στον δημιουργό του περίπου 3 εκατομμύρια δολάρια ετησίως διαφημίζοντας viagra, ήταν υπεύθυνο για το ένα τρίτο του spam παγκοσμίως και το κόστος του για τις εταιρίες ήταν στην πραγματικότητα εκατονταπλάσιο.

Σύμφωνα με την μελέτη του 2019 των Anderson et al. υπάρχουν επιμέρους στοιχεία, για Ευρωπαϊκές χώρες ή και Ηνωμένες Πολιτείες τα οποία μας δίνουν μιας εκτίμηση της συνολικής εικόνας. [18]

Πίνακας Β 0.6 Ετήσια αξία της αγοράς στο Dark web, το έτος 2019

<i>Τύπος</i>	<i>Ετήσια αξία μαύρης αγοράς</i>	<i>Αύξηση/μείωση από 2012</i>
Πιστωτικές κάρτες	731.8 εκατ. λίρες (UK)	Μειωμένο ποσό συναλλαγών
Online τραπεζικές απάτες	121.4 εκατ. λίρες (UK)	Αυξημένα ποσά
POS απάτες	158 εκατ. λίρες	Αυξημένα ποσά
Ransomware	Πολύ πάνω από 10 εκατ. δολάρια	Μεγάλη αύξηση
Cryptocrime	2 δις δολάρια	Δεν υπήρχε
Διαφήμιση	Λίγα δις δολάρια	Όχι αρκετά δεδομένα
Πλαστά antivirus	7.1 εκατ. δολάρια	Μείωση 90%
Ψεύτικη τεχνική υποστήριξη	39 εκατ. δολάρια	Ραγδαία αύξηση
Εταιρικά emails	1.3 δις. δολάρια	
Wannacry/NotPetya	1-2 εκατ. δολάρια	Τυχαία συμβάντα

Κεφάλαιο Γ'

Κατηγορίες κακόβουλου λογισμικού

Η μελέτη των διαφόρων μορφών κακόβουλου λογισμικού, του κόστους αγοράς τους στο σκοτεινό διαδίκτυο, της ζημιάς που επιφέρουν στην αγορά παρουσιάζονται σε αυτό το κεφάλαιο. Εταιρικά στοιχεία που υποκλέπτονται ή κρυπτογραφούνται για λύτρα, βάσεις δεδομένων με στοιχεία πελατών που διατίθενται προς πώληση, διαφημίσεις που ανακατευθύνονται και χειραγωγούνται, ευπάθειες λογισμικού που επιτρέπουν την πρόσβαση σε δίκτυα και υπολογιστικά συστήματα, όλα αυτά πωλούνται σε κατάλληλες τιμές.

Γ.1 Τραπεζικό κακόβουλο λογισμικό (banking malware)

Σύμφωνα με την εταιρία Kaspersky, με βάση στατιστικά δεδομένα από τους πελάτες της, ο τραπεζικός κλάδος δέχτηκε χιλιάδες επιθέσεις στο τρίτο τρίμηνο του έτους 2021, από ιούς που προσβάλλαν servers και POS. Η κατανομή των κακόβουλων προγραμμάτων φαίνεται στον παρακάτω πίνακα:

Πίνακας Γ' 0.1 Κατανομή κακόβουλων προγραμμάτων το πρώτο τρίμηνο του 2021

	Όνομα	Οικογένεια ιογενών προγραμμάτων	%*
1	Zbot	Trojan.Win32.Zbot	17.7
2	SpyEye	Trojan-Spy.Win32.SpyEye	17.5
3	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	9.6
4	Trickster	Trojan.Win32.Trickster	4.5
5	RTM	Trojan-Banker.Win32.RTM	3.6
6	Nimnul	Virus.Win32.Nimnul	3.0
7	Gozi	Trojan-Banker.Win32.Gozi	2.7
8	Danabot	Trojan-Banker.Win32.Danabot	2.4
9	Tinba	Trojan-Banker.Win32.Tinba	1.5
10	Cridex	Backdoor.Win32.Cridex	1.3

Στην πρώτη θέση βρίσκεται η οικογένεια Zeus/Zbot ενώ στην δεύτερη θέση η οικογένεια SpyEye, η οποία είχε μόλις 8.8% ποσοστό το προηγούμενο τρίμηνο. [19]

Γ.2 Ευπάθειες πληροφοριακών συστημάτων (vulnerabilities exploit)

Ένα πολύ σημαντικό και προσοδοφόρο κομμάτι της αγοράς ιομορφικού λογισμικού, είναι η άμεση εκμετάλλευση ευπαθειών διαφόρων εφαρμογών ή υπηρεσιών που εκτελούνται σε προσωπικούς υπολογιστές ή εταιρικούς εξυπηρετητές. Οι εφαρμογές

μπορεί να είναι λειτουργικά συστήματα, λογισμικό προστασίας (antivirus), λογισμικό δικτύων (gateways), βάσεις δεδομένων κ.α. Μόλις ανακαλυφθεί μια ευπάθεια στο εκάστοτε λογισμικό και προτού προλάβει η κατασκευάστρια εταιρία να παρουσιάσει μια διόρθωση (patch), εμφανίζονται κακόβουλα προγράμματα (ιοί) που εκμεταλλεύονται (exploit) την ευπάθεια αυτή. Για όσο διάστημα η ενδιαφερόμενη εταιρία λογισμικού δεν έχει αντιληφθεί την ευπάθεια στο λογισμικό της ή δεν έχει προλάβει ακόμη να παρουσιάσει διορθωτικό λογισμικό, η ευπάθεια αυτή ονομάζεται zero-day exploit.

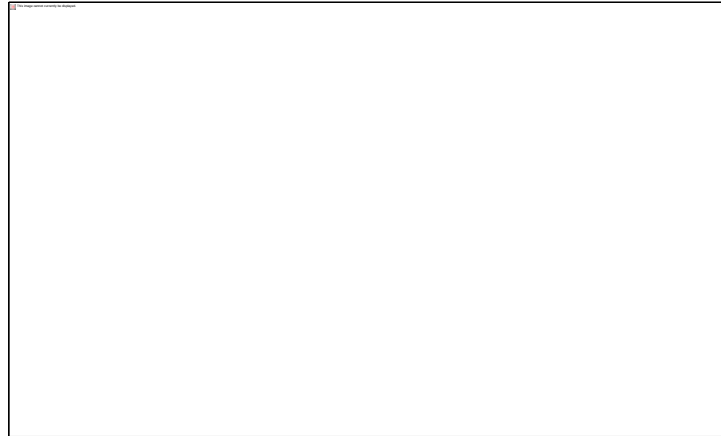
Τα προγράμματα αυτά πωλούνται σε πολύ καλές τιμές, για ένα σύντομο χρονικό διάστημα που συνήθως δεν ξεπερνά τους 3 μήνες, προτού η εταιρίες προλάβουν να παρέχουν το patch και οι πελάτες να εγκαταστήσουν τις απαραίτητες ενημερώσεις.

Το 2015 έγινε αντιληπτό ότι υπήρξε μια αύξηση της πώλησης «ευπαθειών» των windows (exploits) στο dark web. Στην πραγματικότητα οι hackers πωλούσαν κώδικα που εκμεταλλευόταν άγνωστες μέχρι εκείνη την στιγμή ευπάθειες του λειτουργικού συστήματος, με σκοπό να επωφεληθεί κάποιος κακόβουλος χρήστης από την έλλειψη προστασίας. [20]

Σύμφωνα με το παραπάνω, τον Φεβρουάριο του 2015, μια ευπάθεια των Windows ανακαλύφθηκε (CVE-2015-0057) και οι καταναλωτές ενημερώθηκαν από την Microsoft γι' αυτήν. Περίπου ένα μήνα αργότερα, κώδικας που εκμεταλλευόταν αυτή την ευπάθεια βγήκε προς πώληση στο dark web. Αργότερα, τον Ιούλιο του ίδιου έτους ανακοινώθηκε ότι ο Dyre Banking Trojan εκμεταλλευόταν την συγκεκριμένη ευπάθεια για να κλέβει πληροφορίες πιστωτικών καρτών.

Ο ιός μόλυνε το 57,3% των χρηματοπιστωτικών εταιριών παγκοσμίως, εκμεταλλευόμενος την ευπάθεια αυτή των Windows πριν διανεμηθεί η ενημέρωση ασφαλείας από την εταιρία (MS15-010) και υπολογίζεται ότι κόστιζε περίπου 48BTC εκείνη την εποχή (10.000\$ ως 15.000\$ περίπου).

Τον Δεκέμβριο του 2019 (17 Δεκεμβρίου) αποκαλύφθηκε μια ευπάθεια σε δυο προγράμματα της εταιρίας Citrix, τον Application Delivery Controller και το Citrix Gateway. Η ευπάθεια, όπως συμβαίνει συνήθως, επέτρεπε σε κάποιον κακόβουλο χρήστη να εκτελέσει δικό του κώδικα στα συστήματα με τα συγκεκριμένα λογισμικά. Το patch που διόρθωνε το πρόβλημα κυκλοφόρησε στα τέλη Ιανουαρίου 2020.



Εικόνα Γ' 0.1 Επιθέσεις λόγω της ευπάθειας Citrix

Στο διάστημα που μεσολάβησε αλλά και λίγο αργότερα, εκδηλώθηκαν εκατοντάδες χιλιάδες επιθέσεις οι οποίες προσπάθησαν να εκμεταλλευτούν το κενό ασφαλείας (Web Attack: Citrix ADC RCE CVE-2019-19781), με την κορύφωση να έρχεται τον Φεβρουάριο 2020. Τον μήνα αυτό, μόνο η εταιρία Symantec αναφέρει ότι απέτρεψε 492.000 τέτοιες επιθέσεις. [21]

Bug Bounty programs (προγράμματα αμειβόμενης αναφοράς λαθών) ονομάζονται οι προσφορές, πολλών ιστοσελίδων, οργανισμών ή εταιριών ανάπτυξης λογισμικού προς τους hackers, σε χρήμα και άλλα προνόμια, ώστε να αναφέρουν πρώτα σε αυτές τα bugs που βρίσκουν στο λογισμικό τους. Είναι ένας εύσχημος τρόπος να αποτρέψουν την δημιουργία και χρήση ιομορφικού λογισμικού που θα χρησιμοποιηθεί για επιθέσεις εναντίον τους, αφού πληρώνουν πρώτες αυτές όποιον ανακαλύψει και τους αναφέρει μια ευπάθεια.

Ωστόσο τα ποσά που προσφέρουν δεν είναι αρκετά μεγάλα. Εκτιμάται ότι η πώληση προγραμμάτων που εκμεταλλεύονται μια ανακαλυφθείσα ευπάθεια (zero-day exploit) μπορεί να είναι 10 ως 100 φορές μεγαλύτερα από αυτά που προσφέρουν οι εταιρίες. Ο πειρασμός του κέρδους είναι μεγάλος για έναν καλό προγραμματιστή, επομένως υπάρχει πάντα μια αρκετά μεγάλη αγορά στο dark web. Τα λογισμικά που προσφέρονται σε ιστοσελίδες ή forums ποικίλουν (Trojans, virus, worms, Rat, Exploit kit) όπως και οι τιμές τους. [15]

Με το πέρασμα του χρόνου, τέτοιου είδους αγοραπωλησίες γίνονται ολοένα και πιο εύκολες. Οι σύγχρονες πλατφόρμες στο dark web μοιάζουν πολύ με τις νόμιμες, τόσο εμφανισιακά όσο και από άποψη λειτουργίας. Όταν κάποιος αγοράζει ένα προϊόν, μπορεί να αφήσει σχόλια και αξιολόγηση για τον πωλητή και για τον βαθμό ικανοποίησής του από την αγοραπωλησία, την πληρωμή και το τελικό προϊόν. Έτσι οι

πωλητές φτιάχνουν τη φήμη τους και έναν βαθμό αξιοπιστίας προς τους πελάτες, παρόλη την ανωνυμία τους.

Οι πληρωμές γίνονται με κρυπτονομίσματα και η παράδοση των προϊόντων μέσω email ή download links. Πωλητής και αγοραστής διατηρούν την ανωνυμία τους, επιπλέον πληροφορίες που θα αποκάλυπταν την θέση ή το όνομά τους δεν χρειάζεται να ανταλλαχθούν μεταξύ τους. Η αγορά δεν έχει γεωγραφικά σύνορα, αφού δεν χρειάζεται να έρθουν οι δύο πλευρές σε άμεση επαφή ούτε και να μεταφερθεί κάποιο ογκώδες δέμα σε μεγάλες γεωγραφικές αποστάσεις. Αυξάνεται έτσι και το πιθανό κέρδος των πωλητών, αφού απευθύνονται σε ένα παγκόσμιο κοινό αγοραστών από όλα τα μέρη του κόσμου και δεν υπάρχουν μεταφορικά έξοδα ή δασμοί.

Ορισμένοι πωλητές προσφέρουν εγγύηση για τον αριθμό των συστημάτων που θα μπορέσει να μολύνει το προϊόν τους ή και τον χρόνο που θα μείνει κρυμμένο από antivirus προγράμματα. Icepack, Nuclear, LuckySploit, CrimePack είναι ονόματα κάποιων exploit kits που παρουσιάστηκαν παλιότερα. Τα zero-day exploits, παρόλο που είναι πιο κερδοφόρα για τους πωλητές, πωλούνται πολύ πιο δύσκολα για δύο λόγους. Είναι ακριβότερα και η χρήση τους είναι συνήθως πολύ εξειδικευμένη. Επομένως θα πρέπει να βρεθεί αγοραστής που να έχει μια συγκεκριμένη ανάγκη και να μπορεί ταυτόχρονα να διαθέσει τα χρήματα.

Οι δυνατότητες για επιθέσεις DDOS έχουν αυξηθεί δραστικά τα τελευταία χρόνια και οι hackers διαθέτουν πλέον μεγάλα botnets τα οποία μπορούν να διαθέσουν σε κάποιον πελάτη ως υπηρεσία. Ο πελάτης μπορεί να τα χρησιμοποιήσει για spamming, cracking και denial of service επιθέσεις. Η ενοικίαση μπορεί να είναι ωριαία, ημερήσια ή εβδομαδιαία, ανάλογα με της ανάγκες του πελάτη. Συχνά υπάρχουν εγγυήσεις, όπως ότι μια ιστοσελίδα θα βγει εκτός λειτουργίας για 24 ώρες ή περισσότερο.

Παραδείγματα επιθέσεων που εκτελέστηκαν μέσα στο 2021 είναι τα εξής: Το group HelloKitty εκμεταλλεύτηκε την ευπάθεια CVE-2019-7481 που παρουσιάστηκε στις συσκευές SonicWall gateways για να μεταφέρει ransomware λογισμικό ενώ το group LockFile εκμεταλλεύτηκε τις ευπάθειες CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 στον ProxyShell για να αποκτήσουν τον έλεγχο του domain controller και να διεισδύσουν σε ολόκληρα δίκτυα. [19]

Πίνακας Γ' 0.2 Πρόσφατες zero-day exploits

Δεκέμβριος 2020	Accellion FTA επίθεση	CVE-2021-27101, CVE-2021-27104
Δεκέμβριος 2020	SolarWinds Orion Supernova επίθεση	CVE-2020-10148

Ιανουάριος 2021	Accellion FTA επίθεση	CVE-2021-27102, CVE-2021-27103
Μάρτιος 2021	Microsoft Exchange Server επιθέσεις	CVE-2021-26855, CVE-2021-6857, CVE-2021-26858, CVE-2021-27065
Ιούλιος 2021	Kaseya ransomware επίθεση	CVE-2021-30116
Ιούλιος 2021	SolarWinds Serv-U FTP επίθεση	CVE-2021-35211
Ιούλιος 2021	Ευπάθεια των MacOS και iOS που την εκμεταλλεύτηκε το NSO Group	CVE-2021-30807, patched

Γ.3 Malvertising

Η δικτυακή διαφήμιση είναι μια καλοπληρωμένη βιομηχανία, με τζίρο διαρκώς αυξανόμενο. Το συνολικό ποσό υπολογίζεται σε περίπου 267δισ δολάρια το 2018, 290δισ δολάρια το 2019 και 320δισ δολάρια το 2020. Εκατομμύρια διαφημίσεων παρουσιάζονται στους χρήστες του διαδικτύου καθημερινά, κατευθύνοντάς τους σε σελίδες και προϊόντα των διαφημιζομένων. Φυσικό όμως είναι ότι μια τόσο μεγάλη αγορά έχει τραβήξει το ενδιαφέρον κακόβουλων χρηστών, οι οποίοι προσπαθούν να την εκμεταλλευτούν για ίδιον όφελος. Η πιο συνηθισμένη πρακτική τους είναι να παρουσιάζουν στους τελικούς χρήστες δικές τους, μη-ασφαλείς διαφημίσεις, οι οποίες περιέχουν κακόβουλο κώδικα που υποβαθμίζει την ασφάλεια των υπολογιστών των χρηστών ή υποκλέπτουν προσωπικά τους δεδομένα.

Η πρακτική αυτή έχει γίνει γνωστή ως Malvertising, ένα συνδυασμό των λέξεων Malware – Advertising, και το κόστος της εις βάρος της νόμιμης οικονομίας εκτιμάται ότι άγγιξε το 1.1 εκ. δολάρια το 2017. Οι διαφημίσεις αυτές προσθέτουν κακόβουλο κώδικα στον υπολογιστή του χρήστη, ακόμα κι αν αυτός δεν έχει κάποια αλληλεπίδραση με την διαφήμιση που βλέπει. Αρκεί μόνο να ανοίξει μια σελίδα στον φυλλομετρητή του.

Η βιομηχανία της δικτυακής διαφήμισης είναι αρκετά πολύπλοκη και σχηματίζεται από σχέσεις και ανταλλαγές μεταξύ ιστοσελίδων (τις οποίες επισκέπτεται ο χρήστης) και εξυπηρετητών που περιέχουν και προωθούν τις διαφημίσεις. Ο διαφημιστικός χώρος πωλείται σε διαφημιστές και αυτοί αποφασίζουν ποιες και πόσες διαφημίσεις θα φορτωθούν σε κάθε ιστοσελίδα.

Στο σημείο αυτό, κάποιος ικανός hacker μπορεί να παρέμβει και να μεταφέρει σε προσωπικούς υπολογιστές, κακόβουλο λογισμικό. Αγοράζοντας διαφημιστικό χώρο

από κάποιον διαφημιστή, μπορεί να φορτώσει σε κάποιον εξυπηρετητή μια διαφήμιση, μολυσμένη με το κακόβουλο λογισμικό. Όταν ο χρήστης πατήσει πάνω στην διαφήμιση, ο κακόβουλος κώδικας περνάει στον υπολογιστή του. Πολλές φορές αυτό γίνεται αυτόματα, χωρίς να απαιτείται η αλληλεπίδραση του χρήστη με την διαφήμιση.

Λόγω της πολυπλοκότητας της δικτυακής διαφήμισης, ο φυλλομετρητής του χρήστη συχνά ανακατευθύνεται διαδοχικά από κάποιον ad server σε κάποιον άλλο, αφού οι διαφημιστές έχουν συνήθως αγοράσει χώρο σε πολλούς από αυτούς τους servers. Κατά την διαδρομή αυτή, από τον φυλλομετρητή στον ad server, μπορεί να παρέμβει κάποιος και να στείλει κακόβουλο κώδικα στον υπολογιστή του χρήστη.

- Steganography είναι μια τεχνική κατά την οποία ο κακόβουλος κώδικας κρύβεται μέσα σε κείμενα ή εικόνες που θα παρουσιαστούν στον τελικό χρήστη ως διαφημίσεις.
- Polyglot images είναι μια εξέλιξη της παραπάνω τεχνικής, αφού οι εικόνες περιέχουν και τα απαραίτητα scripts για να εκτελεστεί ο κακόβουλος κώδικας που περιέχουν και να ξεκινήσει μια επίθεση.
- Ψεύτικη τεχνική υποστήριξη/scareware όπου pop-up μηνύματα ή κάποιος «τεχνικός» προσπαθεί να πείσει τον χρήστη ότι υπάρχει πρόβλημα με τον υπολογιστή του και πρέπει να πληρώσει για να το λύσει δικτυακά.

Το 2020 οι παραπάνω τεχνικές χρησιμοποιήθηκαν για να προσβάλουν τον Internet Explorer (IE) με πρόσχημα τον ιό Covid-19. Η επίθεση χρησιμοποίησε το Fallout exploit kit για να προσβάλουν υπολογιστές που χρησιμοποιούσαν τον «παροπλισμένο» φυλλομετρητή (IE) για να προβάλλει μια ψεύτικη συμβουλή-ενημέρωση με θέμα τον Covid-19. Στόχος τους ήταν να κλέψουν προσωπικά δεδομένα και κωδικούς.

Το 2015 ο Edward Snowden ενθάρρυνε την χρήση ad blockers για να αποτραπεί το malvertising. «Αφού κάποιος παρουσιάζουν διαφημίσεις που έχουν ενεργό περιεχόμενο το οποίο απαιτεί την χρήση javascript για να παρουσιαστεί ή περιέχει ενσωματωμένο Flash κώδικα ή οποιονδήποτε άλλο κώδικα που μπορεί να επιτεθεί στον φυλλομετρητή σας, καλό είναι να κάνετε ότι μπορείτε για να το μπλοκάρετε» . [22]

Ένα τμήμα του malvertising μπορεί να θεωρηθεί και το spam messaging, δηλαδή η αποστολή διαφημιστικών μηνυμάτων στα email ανυποψίαστων χρηστών. Για να το πετύχουν, οι διαφημιστικές εταιρίες αγοράζουν «πακέτα» διευθύνσεων, τα οποία οι hackers έχουν μαζέψει από διάφορες πηγές, όπως βάσεις δεδομένων τραπεζών, δημόσιων οργανισμών, νοσηλευτικών ιδρυμάτων ή ηλεκτρονικών καταστημάτων.

Το κόστος ποικίλει, συνήθως όμως προσεγγίζει τα 100\$ για κάθε 100.000 προσωπικές διευθύνσεις. Οι διευθύνσεις email ομαδοποιούνται σε πακέτα τα οποία μπορεί να έχουν κάποια κοινά χαρακτηριστικά, όπως η ηλικία ή η χώρα προέλευσης.



Εικόνα Γ' 0.2 Πώληση υπηρεσιών malvertize στο Dark web

Πιο ακριβά πωλούνται τα εταιρικά emails που μπορεί να έχει υποκλέψει κάποιος, καθώς προσφέρονται για περισσότερες απάτες που μπορεί να στοχεύουν τόσο τον υπάλληλο όσο και το λογιστήριο της εταιρίας. Μια συνηθισμένη απάτη είναι, αφού διαβάσει κάποιος ένα νήμα μηνυμάτων μεταξύ του υπαλλήλου και του λογιστηρίου της εταιρίας, το οποίο περιέχει αποδείξεις πληρωμής, να προσπαθήσει να αλλάξει τον λογαριασμό πληρωμής του υπαλλήλου.

Γ.4 Ransomware

Σύμφωνα με την ετήσια αναφορά της εταιρίας κυβερνο-ασφάλειας CrowdStrike Inc., το 63% των επιθέσεων του έτους 2020 είχαν οικονομικά κίνητρα. Από αυτές τις επιθέσεις η συντριπτική πλειοψηφία (81%) αφορούσε ransomware, ενώ το υπόλοιπο ποσοστό (19%) είχε να κάνει με επιθέσεις σε ηλεκτρονικά καταστήματα, υποκλοπή εταιρικών email και εξόρυξη κρυπτονομισμάτων. [23]

Το Ransomware είναι κακόβουλο λογισμικό που ζητάει λύτρα, αφού πρώτα καταφέρει να στερήσει από κάποιον χρήστη την πρόσβαση σε υπολογιστή ή στα αρχεία του. Η τεχνική αυτή ανάγεται στην δεκαετία του 1980, ωστόσο σήμερα οι επιτιθέμενοι hackers στοχεύουν προσωπικούς υπολογιστές, εταιρίες ή οργανισμούς, χρησιμοποιούν σύγχρονη κρυπτογράφηση αρχείων και ζητούν τα λύτρα σε κρυπτονομίσματα.

Σε κάποιες περιπτώσεις οι κατασκευαστές του κακόβουλου κώδικα πωλούν την υπηρεσία μαζί με άλλους χρήστες, φαινόμενο που είναι γνωστό σήμερα ως Ransomware-as-a-Service (RaaS).

Οι τρόποι για να μεταφερθεί ο κακόβουλος κώδικας στον υπολογιστή του χρήστη είναι μέσω Malspam, Malvertising, Spear fishing (ψάρεμα) ή social engineering. Αφού ολοκληρωθεί η μεταφορά, η ενεργοποίηση του κώδικα γίνεται συνήθως από το ίδιο το θύμα, με το πάτημα σε κάποιον σύνδεσμο ή το άνοιγμα ενός συνημμένου εγγράφου. Τότε τα αρχεία του κρυπτογραφούνται και χάνει κάθε πρόσβαση σε αυτά ενώ εμφανίζεται ένα μήνυμα που ζητάει λύτρα για την αποκρυπτογράφησή τους.

Τα τελευταία χρόνια, ιδιαίτερα μετά το έτος 2014 και τον CryptoLocker, στόχος του ransomware έχουν γίνει και τα κινητά τηλέφωνα. Το έτος 2016 εμφανίστηκε το πρώτο ransomware λογισμικό για MacOS. Ονομαζόταν KeRanger και πρόσβαλλε μια εφαρμογή που ονομαζόταν Transmission. Όταν εκτελούνταν η εφαρμογή, πολλά αντίγραφα του κακόβουλου κώδικα εκτελούνταν στο background για διάστημα μέχρι και τρεις ημέρες, προτού ενεργοποιηθούν και αρχίσουν να κρυπτογραφούν αρχεία.

Πολύ σύντομα βγήκε μια ενημέρωση για το σύστημα ασφαλείας XProtect της Apple που απέτρεπε πλέον την εκτέλεση του κακόβουλου κώδικα. Ωστόσο το έτος 2017 ακολούθησαν δύο ακόμα προγράμματα με στόχο το MacOS, τα Findzip και MacRansom.

Τα τελευταία χρόνια το Ransomware στρέφεται προς τις μεγάλες εταιρίες. Παρόλο που αρχικά είχε ως κύριο στόχο τους οικιακούς χρήστες, γρήγορα έγινε κατανοητό από τους hackers ότι μεγαλύτερες προοπτικές υπήρχαν στο χώρο των εταιρικών υπολογιστών. Με κίνδυνο να σταματήσει η παραγωγή τους ή να χάσουν χρήσιμα εταιρικά αρχεία οι εταιρίες ήταν διατεθειμένες να πληρώσουν μεγάλα ποσά.

Στο τέλος του 2016, το 12.3% των επιθέσεων σε εταιρίες ήταν ransomware, ενώ στους προσωπικούς υπολογιστές ήταν μόλις 1.8%. Το 2017 το 35% των μικρών και μεσαίου μεγέθους εταιριών είχαν υποστεί επιθέσεις ransomware. Την εποχή της πανδημίας, δηλαδή το 2020, οι επιθέσεις στράφηκαν σε νοσοκομεία και ιδιωτικές κλινικές, ενώ η

απειλή προς αυτές ήταν διπλή : καταστροφή των ευαίσθητων ιατρικών δεδομένων ή διαρροή τους.

Οι επιθέσεις αυτού του τύπου γίνονται όλο και πιο συχνές τα τελευταία δύο χρόνια, από τις αρχές του 2019 κι έπειτα, μάλιστα έχουν ονομαστεί *επιθέσεις δυσφήμισης* (name-and-shame attacks) διότι στο θύμα τίθεται ένα διπλό δίλημμα, που έχει να κάνει με την καλή φήμη του. Από την μία πλευρά να ανακτήσει τα δεδομένα που οι hackers έχουν κρυπτογραφήσει (availability) και από την άλλη να αποτρέψει την δημοσίευσή τους στο διαδίκτυο (confidentiality).

Για κάποιες εταιρίες, η δημοσίευση ευαίσθητων δεδομένων μπορεί να είναι σημαντικότερο χτύπημα από την αποκατάσταση των κρυπτογραφημένων δεδομένων τους. Η πίεση από τους επιτιθέμενους αυξάνεται όταν θέτουν deadlines, δηλαδή χρονικό περιορισμό για την καταβολή της πληρωμής, προτού δημοσιεύσουν τα κλεμμένα δεδομένα. [24]

Οι κυριότερες αγορές που πλήττονται από επιθέσεις ransomware είναι των ΗΠΑ, Βρετανίας και Καναδά, ενώ ακολουθούν οι αναπτυσσόμενες αγορές της Ασίας και της Λατινικής Αμερικής. Τα προγράμματα ransomware είτε πωλούνται σε άτομα που θέλουν να τα χρησιμοποιήσουν κατά μόνας, πραγματοποιώντας μικρού μεγέθους επιθέσεις, είτε χρησιμοποιούνται από ομάδες κακόβουλων χρηστών (hack groups) για την πραγματοποίηση μεγάλου μεγέθους επιθέσεων.

Το κόστος για προγράμματα ransomware ποικίλει, από 50\$ μέχρι και 500\$. Ο τρόπος λειτουργίας του και η ποιότητα της κρυπτογράφησης, επηρεάζουν το κόστος. Συνήθως πρόκειται για ένα αρχείο .exe στο οποίο ο πωλητής έχει βάλει τα στοιχεία που επιθυμεί ο αγοραστής, όπως ένα κατάλληλο μήνυμα λύτρων και το κατάλληλο πορτοφόλι για την πληρωμή τους. Παρέχεται επίσης και το κλειδί αποκρυπτογράφησης. Επειδή τα αρχεία αυτά ανιχνεύονται από τα antivirus, ο πωλητής μπορεί να το παρέχει κρυπτογραφημένο, με το ανάλογο κόστος, διαφορετικά πρέπει ο πελάτης να το κρυπτογραφήσει ο ίδιος.



Εικόνα Γ' 0.3 Πώληση υπηρεσιών ransomware as a service

Πολλές ιστοσελίδες παρέχουν και την αντίστροφη υπηρεσία, δηλαδή την αποκρυπτογράφηση αρχείων σε υπολογιστές που έχουν δεχθεί επίθεση ransomware. Εδώ το κόστος είναι προφανώς μικρότερο, φτάνοντας μέχρι τα 250\$, ώστε να είναι μικρότερο από τα «λύτρα» που πιθανόν ζητούνται. Για να αποκρυπτογραφηθούν τα αρχεία, θα πρέπει ο πελάτης να τους παρέχει συγκεκριμένα αρχεία και μετά από λίγες ώρες (8 ως 12) θα λάβει το κλειδί αποκρυπτογράφησης. Φυσικά ο κάθε hacker ισχυρίζεται ότι δεν θα ξεκλειδώσει υπολογιστή που έχει κρυπτογραφηθεί με εργαλείο ransomware που έχει δημιουργήσει ο ίδιος.



Εικόνα Γ' 0.4 Στιγμιότυπο από υπολογιστή που έχει δεχθεί επίθεση ransomware

Σύμφωνα με την εταιρία Kaspersky, στο τρίτο τρίμηνο 2021, στις αρχές Ιουλίου 2021 εκδηλώθηκε μια μεγάλη επίθεση ransomware, μέσω του λογισμικού απομακρυσμένης

διαχείρισης Kaseya VSA. Το hack group REvil/Sodinokibi κατάφερε να κλειδώσει πάνω από 1000 πελάτες εταιριών που χρησιμοποιούσαν το λογισμικό αυτό, ζητώντας λύτρα 70 εκ. δολαρίων. Μετά από αυτό, οι αρχές έστρεψαν την προσοχή τους στο REvil group, το οποίο γρήγορα εγκατέλειψε την υποδομή που είχε δημιουργήσει, σταμάτησε τις νέες μολύνσεις και εξαφανίστηκε. Η εταιρία Kaseya απέκτησε ένα κλειδί αποκρυπτογράφησης, το οποίο παρείχε σε όλους τους πελάτες της ώστε να ξεκλειδώσουν τα δεδομένα τους. Σύμφωνα με την δήλωση της εταιρίας, απέκτησε το κλειδί από το FBI και δεν πλήρωσε λύτρα, ούτε απευθείας ούτε μέσω τρίτων.

Την ίδια περίπου στιγμή, η Europol και η Ουκρανική αστυνομία συνέλαβαν δύο μέλη hack group που δεν κατονομάστηκε, τα οποία συμμετείχαν σε επιχείρηση ransomware αξίας 5 ως 70 εκ. δολαρίων. [19]

Νωρίτερα, τον Φεβρουάριο του 2021, η εταιρία KIA motors δέχθηκε επίθεση με το λογισμικό DoppelPaymer, τον διάδοχο του λογισμικού BitPaymer, και ζητήθηκαν λύτρα 20εκ δολαρίων. Το hack group που οργάνωσε την επίθεση, απείλησε να δημοσιοποιήσει τα δεδομένα της εταιρίας μετά από 3 εβδομάδες, αν δεν εισέπραττε τα λύτρα που ζητούσε. Εκτός από την απώλεια των δεδομένων, η επίθεση προκάλεσε μεγάλο πρόβλημα στις υποδομές της εταιρίας, στις πληρωμές και στην παράδοση νέων αυτοκινήτων στους εμπόρους. [25]

Πίνακας Γ' 0.3 Τα πιο γνωστά ransomware λογισμικά των τελευταίων ετών

- | | | | |
|----------------|----------------|----------------|----------|
| • BadRabbit | • Dharma | • Maze | • Petya |
| • BitPaymer | • DoppelPaymer | • MeduzaLocker | • REvil |
| • Cerber | • GandCrab | • NetWalker | • Ryuk |
| • Cryptolocker | • Locky | • NotPetya | • SamSam |
| • WannaCry | | | |

Οι ομάδες κακόβουλων χρηστών υιοθετούν χαρακτηριστικά ονόματα για μικρό συνήθως χρονικό διάστημα, πριν εξαφανιστούν ή μετονομαστούν. Τα τελευταία 2 χρόνια υπήρξαν οι ομάδες Gold Village (Maze), Gold Herron (DoppelPaymer), Gold Southfield (REvil), Gold Mansard (Nemty) κ.α. Από τον Μάρτιο 2020 μέχρι τον Ιούνιο 2021 οι ομάδες που εμφανίστηκαν σε επιθέσεις ήταν τουλάχιστον 27.

Κάποιες από τις ομάδες αυτές πρόσθεσαν στο ρεπερτόριό τους και εκδόσεις γνωστών ransomware, που χτυπούν Linux μηχανήματα, όπως 777, Babuk, HelloKitty, REvil και DarkSide. [24]

UNKN
gigabyte
□□□□

Seller
□ thirty
124 posts
Joined
04/07/19 (ID:94090)

Posted May 8 (edited)
Report post □
Added Linux version. Cryptography is ported from the Windows version, so everything is also reliable, unlike third-party solutions. It will also work on NAS if its architecture is x86-x64, and the kernel is version 3.0 or higher. More details can be found in NEWS.
1 domain available.
Edited Sunday at 12:14 PM by UNKN

□ Quote
React

Εικόνα Γ' 0.5 Φόρουμ διαφημίζει την Linux έκδοση του REvil

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted. No free decryption software is available in the public. Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.

- Your reference ID: **31**
(we recommend to put the reference ID as the subject when contacting us)
- BTC wallet for payment:


REDACTED

REDACTED

you can check the status here: <https://blockchain.info/address/>

REDACTED
- Contact email:

REDACTED

To get the files in your network decrypted you should pay for the decryption software. The price for the decryptor is based on the network size, number of employees, annual revenue. Please feel free to contact us for amount of BTC should be paid.

Some sensitive information was stolen from the file servers and will be uploaded in the public in case you won't pay us.

You should get in contact with us within 3 days after you noticed the encryption. If this doesn't happen the price is doubled after 3 days passed.

You should pay within 7 days since we receive the first email from you. If this doesn't happen the price is doubled after 7 days since first email.

Εικόνα Γ' 0.6 Το λογισμικό BitPaymer (πρόγονος του DoppelPaymer) σε δράση

Δυστυχώς τα στοιχεία που να δείχνουν τον ακριβή αριθμό επιθέσεων που διενέργησε το κάθε hack group, όπως και το λογισμικό ransomware που χρησιμοποιήθηκε σε κάθε επίθεση, είναι ελλιπή και δύσκολο να διασταυρωθούν, ακριβώς λόγω της μυστικότητας των επιθέσεων. Ένα παράδειγμα που δείχνει το μέγεθος της διαφοράς ανάμεσα στις πραγματικές επιθέσεις και σε αυτές που ανακοινώνονται δημοσίως, αναφέρεται στην ετήσια έκθεση της εταιρίας Secureworks.

Στον παρακάτω πίνακα φαίνονται τα ransomware γκρουπ που λειτουργούσαν τον Ιούνιο 2021, το πλήθος των δημοσιευμένων θυμάτων που είχαν μέχρι τότε, από την πρώτη ημέρα εμφάνισής τους, βασισμένα σε στοιχεία διαρροών.

Ransomware	Ημερομηνία πρώτης επίθεσης	Συνολικές ημέρες λειτουργίας	Πλήθος δημοσιευμένων θυμάτων	Μέσο πλήθος θυμάτων ανά 30 ημέρες
Conti	2019-11-29	570	417	22
Maze	2019-12-07	334	266	24
REvil	2019-05-01	782	259	10
Egregor	2020-09-18	103	206	60
DoppelPaymer	2019-07-02	720	200	8
Pysa	2019-10-11	619	189	9
Avaddon	2020-06-01	373	182	15
NetWalker	2019-09-05	509	144	8
Darkside	2020-08-01	285	99	10
Clop	2019-02-01	871	65	2
Babuk	2021-01-04	168	43	8
LV	2021-04-09	73	40	16
Netfilm	202-03-14	464	40	3
Everest	2020-12-01	202	39	6
Prometheus	2021-03-28	85	37	13
Ragnarok	2020-01-01	537	33	2
Marketo	2021-04-13	69	32	14
RagnarLocker	2020-02-04	503	27	2
Suncrypt	2020-08-25	300	22	2
RansomExx	2020-06-17	369	21	2
Mount Locker	2020-07-1	355	20	2
Xing	2021-04-29	53	18	10
Lorenz	2021-04-29	53	17	10
Astro Team	2021-03-02	111	16	4
Grief	2021-05-27	25	15	Δεν ορίζεται
AKO	2020-01-09	181	9	1
Cuba	2020-12-01	202	9	1
LockBit	2019-10-19	611	9	0
Sekhmet	2020-03-18	103	6	2
Snatch	2019-05-01	16	6	Δεν ορίζεται
NoName	2021-04-28	54	6	3
SynACK	2021-03-28	85	6	2
Ranzy	2020-08-18	307	3	0
Payload bin	2021-05-31	21	2	Δεν ορίζεται

Ransomware	Ημερομηνία πρώτης επίθεσης	Συνολικές ημέρες λειτουργίας	Πλήθος δημοσιευμένων θυμάτων	Μέσο πλήθος θυμάτων ανά 30 ημέρες
Nemty	2020-03-03	1	1	Δεν ορίζεται

Τα πιο παλιά και οργανωμένα γκρουπ έχουν δημοσιεύσει τα πιο πολλά θύματα. Πιθανότατα δεν είναι η πραγματική εικόνα όλων των θυμάτων, προφανώς οι επιθέσεις στις οποίες πληρώθηκαν λύτρα εκ μέρους του θύματος, δεν φαίνονται στον πίνακα. Μία χαρακτηριστική περίπτωση από την οποία προκύπτει το παραπάνω συμπέρασμα είναι η περίπτωση του γκρουπ Avaddon.

Το γκρουπ Avaddon δημοσίευσε τον Ιούνιο 2021 μια λίστα με 182 επιθέσεις, από την αρχή της δράσης του τον Ιούνιο 2020. Ωστόσο όταν το γκρουπ τερμάτισε την λειτουργία του, δημοσίευσε 2.934 διαφορετικά κλειδιά αποκρυπτογράφησης, το καθένα από τα οποία αντιστοιχούσε σε μια επιτυχημένη επίθεση. Αυτό σημαίνει ότι οι πραγματικοί αριθμοί ήταν 16 φορές μεγαλύτεροι από ότι εικάζονταν, όταν το γκρουπ ήταν ενεργό.

Ο στόχος μιας επίθεσης δεν είναι πάντα προκαθορισμένος. Τα στοιχεία δείχνουν ότι οι hackers καιροφυλακτούν ώστε να βρουν εύκολη αρχική πρόσβαση σε ένα δίκτυο ή υπολογιστικό σύστημα και αφού αποκτήσουν και διατηρήσουν τον έλεγχο και εγκαταστήσουν τα απαραίτητα εργαλεία, τότε εκδηλώνουν οργανωμένη επίθεση. [24]

Γ.5 Database leak

Πολύ συχνά οι hackers καταφέρνουν να υποκλέψουν μια ολόκληρη βάση δεδομένων, που περιέχει τα στοιχεία των πελατών μιας εταιρίας ή ενός οργανισμού. Τα δεδομένα αυτά πωλούνται στην συνέχεια στην μαύρη αγορά του dark web, σε περιορισμένα αντίγραφα.

Ανάλογα με το είδος της εταιρίας τα στοιχεία μπορεί να περιέχουν και ευαίσθητα προσωπικά δεδομένα, όπως ιατρικό ιστορικό, οικονομική κατάσταση, επαγγελματικά τηλέφωνα και email, αριθμούς πιστωτικών καρτών κ.α. Συνήθως η βάση δεδομένων πωλείται ολόκληρη και είναι ευθύνη του πελάτη να βρει τρόπο να την αξιοποιήσει.

Η διαρροή (leak) μιας βάσης είναι σημαντική απώλεια για κάθε οργανισμό, γι' αυτό και συνήθως προστατεύεται αρκετά καλά. Αν διαρρεύσει όμως, η τιμή που πετυχαίνουν οι hackers είναι αρκετά μεγάλη. Μπορεί να κυμαίνεται από 150\$ ως 1500\$. Συνήθως οι τιμές ξεκινούν από πολύ ψηλά, για τον πρώτους έναν ή δύο μήνες

και μειώνονται σταδιακά. Πωλούνται όμως και διαρροές αρκετά παλιές, σε χαμηλές βεβαίως τιμές.

Πίνακας Γ' 0.4 Τιμές βάσεων που έχουν διαρρεύσει (leaks) τον Ιανουάριο 2022

Leaked database	Ημερομηνία	Τιμή	Αγορά
nationaleatingdisorders.org Full Database dump	2020	149\$	
000webhost Email addresses, IP addresses, Names, Password	2015	89\$	
Full 143Vpn Database		77\$	
forum 1337-crew.to	2013	79\$	
Webkinz.com Database	2020	99\$	
Department Of health of a state on US database		600\$	
Full and Complete Original Abandonia Database		79\$	
Major indian cryptocurrency trading platform WazirX, CoinDCX and Unocoin data leak.	Ιανουάριος 2022	1500\$	Dark Leak Market
US Cellular data leak	Δεκέμβριος 2021	800\$	
T Mobile Data Leak Dec-2021	Δεκέμβριος 2021	1000\$	Dark Leak Market
Facebook.com	Ιανουάριος 2022	573\$	Hacked databases
LinkedIn	Ιανουάριος 2022	280\$	Hacked databases
Georgian (Country) Citizenship Database	Ιανουάριος 2022	36\$	Hacked databases

Πίνακας Γ' 0.5 Διευθύνσεις για αγορές βάσεων δεδομένων (leaks)

Dark Leak Market	http://ydnvjy3hfvnmhkf7ayjhfttfamanpyholz2he4sejeokk3ot5ms4fa5ad.onion/
Pay2Key Leak Directory	http://pay2key2zkg7arp3kv3cuugdaqwuesifnbofun4j6yjd5ry7zw2asid.onion/
Arvin club	http://3kp6j22pz3zkv76yutctosa6djpj4yib2icvdqxucdaxxedumhqiicpad.onion/?cat=1
Digital Thrift shop	http://kw4zlnfhxje7top26u57iosg55i7dzuljjcyswo2clgc3mdliviswwyd.onion/
Hacked databases store	http://hackedabm6ejvmh7xiiqddq3ptflorhdvjurhheqbovl64xi3zbrlpad.onion/

Για να ολοκληρωθεί η αγορά, θα πρέπει πρώτα να γίνει η πληρωμή. Η τιμή δίνεται σε κρυπτονόμισμα (bitcoin) αλλά φαίνεται και το ισόποσο σε δολάρια. Όταν γίνει η πληρωμή σε συγκεκριμένο portfolio, ακολουθεί η επιβεβαίωση της από τον ιδιοκτήτη του πορτοφολιού. Μετά από τρεις διαδοχικές επιβεβαιώσεις της πληρωμής,

εμφανίζεται στον πελάτη ένας σύνδεσμος ή ενεργοποιείται ένας ήδη υπάρχων, ώστε να κατεβάσει το προϊόν που αγόρασε.

Database	GameSalad Database
Records	1,499,335 rows
Price	\$30 / 0.0006996 BTC
Download link	gamesalad_database.7z [68.63 MB] make payment to activate link

Transfer **0.0006996 BTC** to address:

1GQxJpCMFtup4qBbEBu9CiHXfK7LbwqYJT



Confirmations: 0

Εικόνα Γ' 0.5 Πληρωμή για αγορά μιας βάσης δεδομένων στο Dark web

Για να αποδείξει ο πωλητής ότι διαθέτει την βάση που διαφημίζει, μπορεί να προσφέρει κάποιο τμήμα της ως δείγμα, στους υποψήφιους αγοραστές που θα επικοινωνήσουν μαζί του. Επειδή όμως και αυτή η διαδικασία είναι χρονοβόρα και μπορεί να προδώσει την ασφάλεια του πωλητή, ορισμένοι από αυτούς πωλούν και το δείγμα.

Με τον τρόπο αυτό ίσως να αποτρέπουν χρήστες που δεν ενδιαφέρονται πραγματικά από το να επικοινωνούν μαζί τους αλλά ταυτόχρονα ελέγχουν και την δυνατότητα του πελάτη να πληρώσει με ασφάλεια.

Στις αρχές Απριλίου 2022 η Europol κατάφερε να συλλάβει τον διαχειριστή της σελίδας Raid Forums καθώς και δύο συνεργούς του. Η σελίδα είχε ως αντικείμενο την πώληση βάσεων δεδομένων που είχαν διαρρεύσει, κυρίως από εταιρίες με έδρα τις ΗΠΑ. Οι βάσεις αυτές περιείχαν κυρίως αριθμούς πιστωτικών καρτών, αριθμούς τραπεζικών λογαριασμών και στοιχεία web-banking για εκατομμύρια υπαλλήλους των εταιριών αυτών.

Η σελίδα αυτή λειτουργούσε από το 2015 και θεωρούνταν από τα μεγαλύτερα Hacking Forums με περισσότερους από μισό εκατομμύριο χρήστες.

Γ.6 Botnets – Loaders

Ένα σημαντικό κομμάτι κάθε επίθεσης είναι ο τρόπος με τον οποίο μπορεί κάποιος να διεισδύσει σε ένα υπολογιστικό σύστημα. Υπεύθυνα γι' αυτό είναι προγράμματα που ονομάζονται Loaders, τα οποία θα εγκατασταθούν σε ένα υπολογιστικό σύστημα μέσω spam email, spear phishing, chat, sms και θα χρησιμοποιηθούν για να εγκαταστήσουν ransomware ή cryptominers. Τα πιο γνωστά από αυτά είναι τα Emotet, IcedID, Chanitor, Cutwail, Dridex, QakBot, Flubot, Teabot αλλά υπάρχουν και πολλά ακόμη.

Τον Ιανουάριο 2021 το Emotet εξαφανίστηκε οριστικά, μετά από συντονισμένες προσπάθειες των αρχών πολλών Ευρωπαϊκών χωρών και του Καναδά. Ωστόσο το κενό που άφησε, γρήγορα καλύφθηκε από άλλα botnets, με κυρίαρχα τα TrickBot, QakBot. Ενώ η συνεργασία των εταιριών με τις διωκτικές αρχές έφερε σημαντικά αποτελέσματα, γρήγορα έγινε αντιληπτό ότι είναι αρκετά δύσκολο να δοθούν μακροπρόθεσμες λύσεις στο πρόβλημα των loaders.

Όπως ακριβώς οι διωκτικές αρχές μελετούν τα botnets, έτσι και οι δημιουργοί τους μελετούν τεχνικές λεπτομέρειες ώστε να κάνουν τα botnets πιο ανθεκτικά. Ως παράδειγμα μπορούμε να αναφέρουμε ότι την ημέρα που οι αρχές κυνήγησαν το Emotet, παρατηρήθηκε μια άμεση αλλαγή στις ρυθμίσεις του Qakbot που χειριζόταν η ομάδα Gold Lagoon. Κύριος σκοπός των αλλαγών ήταν η μεταφορά της υποδομής της ομάδας εκτός Δυτικής Ευρώπης, σε περιοχές όπως η Ρωσία, ώστε να αποφύγουν την επίθεση των αρχών.

Σε πολλές περιπτώσεις οι δημιουργοί των botnets αλλάζουν συχνά γλώσσα προγραμματισμού, για να γράψουν διαφορετικές παραλλαγές τους και να δυσκολέψουν έτσι τον εντοπισμό. Ο Buer loader που είναι γραμμένος σε C πλέον έχει και μια παραλλαγή γραμμένη σε Rust. Ο Nimzaloader είναι εξαρχής γραμμένος σε γλώσσα Nim.

Επιπλέον οφέλη που αποκομίζουν χρησιμοποιώντας νέες γλώσσες προγραμματισμού είναι η προσθήκη νέων δυνατοτήτων, η αποφυγή και ματαίωση των συστημάτων ανάλυσης κακόβουλου λογισμικού αλλά και η ανανέωση παλιότερου malware μέσα από συγγραφή του εξαρχής.

Μια άλλη αλλαγή προέρχεται από την αύξηση των mobile botnets, κυρίως το FluBot και το TeaBot. Η διακίνησή τους γίνεται κυρίως μέσω γραπτών μηνυμάτων, οπότε η μέθοδος ονομάζεται sms phishing ή smishing. Η αύξηση του ηλεκτρονικού εμπορίου λόγω της πανδημίας του Covid-19, έδωσε την ευκαιρία στους hackers να στέλνουν

ψεύτικα μηνύματα αποτυχίας παράδοσης ενός δέματος. Σε αυτά ο ανυποψίαστος χρήστης καλούνταν να πατήσει σε έναν σύνδεσμο, για να κατεβάσει μια φαινομενικά νόμιμη εφαρμογή της εταιρίας παράδοσης.

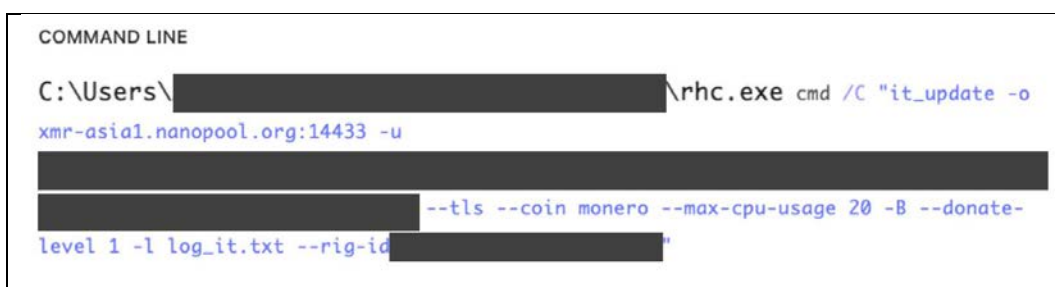
Μετά την εγκατάστασή της, η εφαρμογή εγκαθιστούσε το FluBot και έκλεβε προσωπικά δεδομένα του χρήστη της κινητής συσκευής, τραπεζικά δεδομένα, τις επαφές και τους αποθηκευμένους κωδικούς του. Ο κυριότερος στόχος ήταν συσκευές με android και λιγότερο το iOS.

Γ.7 Cryptojacking

Με την τιμή του bitcoin και άλλων κρυπτονομισμάτων σε ιστορικά υψηλά μέσα στο 2021, οι επιθέσεις αυτού του τύπου αυξήθηκαν σημαντικά κατά την διάρκεια του έτους. Παρόλο που δεν φαίνονται να έχουν ακόμη μεγάλο οικονομικό αντίκτυπο στην αγορά, μακροπρόθεσμα μπορεί να αποτελέσουν πρόβλημα για την αγορά.

Ο στόχος τους μπορεί να είναι διπλός. Αφενός μπορούν να αλλάζουν ηλεκτρονικά πορτοφόλια, ανακατευθύνοντας σημαντικά ποσά κρυπτονομισμάτων προς άλλους λογαριασμούς, αφετέρου έχουν την δυνατότητα να εκτελούν κώδικα σε κάποιο υπολογιστικό σύστημα, επομένως μπορούν να χρησιμοποιηθούν ως loaders για εγκατάσταση ransomware λογισμικού.

Ένας άλλος υπαρκτός κίνδυνος είναι να εγκατασταθούν σε cloud servers και να ξεκινήσουν cryptomining προς όφελος ενός hack group, προκαλώντας έτσι τεράστιο κόστος λόγω της χαμένης υπολογιστικής ισχύος στις εταιρίες.

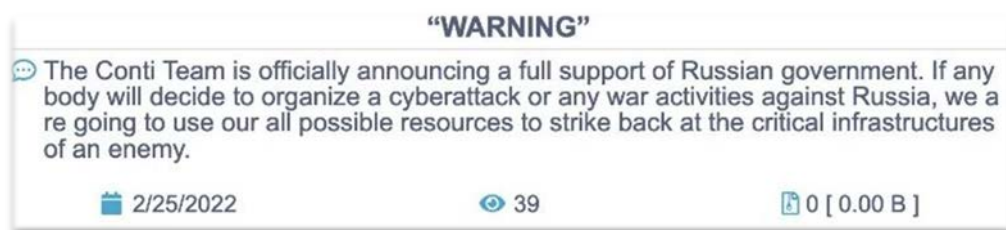


Εικόνα Γ' 0.6 Monero miner που εκτελείται κρυφά μέσω προγράμματος hidec

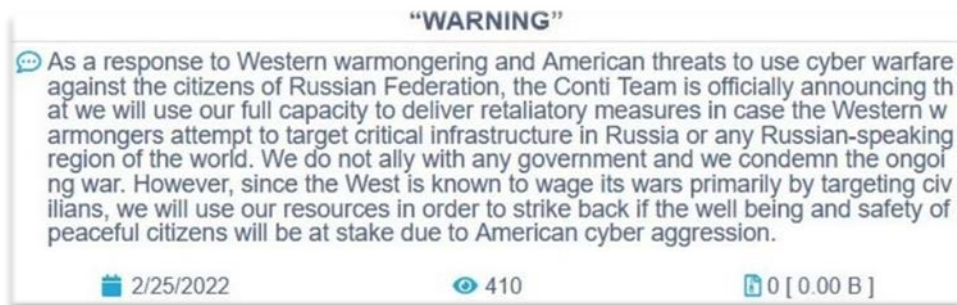
Γ.8 Διαρροή δεδομένων του group Conti.

Το γκρούπ Conti είναι ένα από τα πιο διάσημα ransomware γκρούπ της εποχής μας, έχοντας περισσότερες από 600 επιτυχημένες επιθέσεις μέσα στο 2021 και ένα συνολικό αποθεματικό περίπου 2.3 δις δολαρίων σε κρυπτονομίσματα.

Ένα τόσο μεγάλο γκρουπ που υιοθετεί το μοντέλο RaaS, είναι προφανές ότι απασχολεί πολλά και διαφορετικά μέλη, ίσως και από διαφορετικές γεωγραφικές περιοχές. Με την έναρξη του πολέμου στην Ουκρανία, στις 25/2/2022 το γκρουπ θα μπορούσε να διατηρήσει ουδετερότητα ή να διαλέξει πλευρά. Όταν το έκανε, επιλέγοντας να συνταχθεί με την Ρωσική πλευρά, άρχισε μια σειρά ενεργειών εναντίον του, η οποία οδήγησε σε μια μεγάλου μεγέθους διαρροή των μελών και των εργαλείων του γκρουπ.



Η ανακοίνωση τροποποιήθηκε λίγη ώρα αργότερα ως εξής:



Παρόλο που, όπως υποψιαζόταν ήδη πολλοί, τα μέλη του γκρουπ εδράζονταν στην Ρωσία, φαίνεται ότι κάποια μέλη ήταν Ουκρανοί. Έτσι δυο ημέρες μετά την ανακοίνωση, στις 27 Φεβρουαρίου, ένας ερευνητής ασφαλείας, πιθανότατα ένα πρώην μέλος του γκρουπ που δεν συμφωνούσε με την απόφαση αυτή, ξεκίνησε μια σειρά από διαρροές (leaks) με στοιχεία που είχε συγκεντρώσει τα προηγούμενα δύο χρόνια.

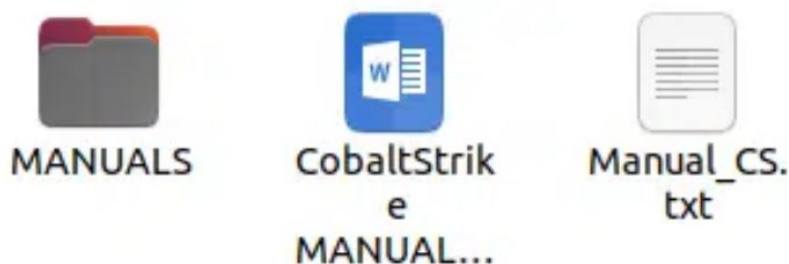
Ξεκίνησε ανοίγοντας έναν λογαριασμό στο twitter με όνομα conti leaks (@contileaks) όπου δημοσίευσε παλιότερες ενέργειες του γκρουπ, chat history, source code των εργαλείων, πρόγραμμα εκπαίδευσης, οδηγίες προς τα μέλη και – το κυριότερο – τον πηγαίο κώδικα για το κακόβουλο λογισμικό του γκρουπ.

Οι διαρροές αποκάλυψαν την καθημερινή εργασία των μελών του γκρουπ, επικοινωνία με τα θύματα, συζητήσεις για επόμενες επιθέσεις, συνεργασία με γκρουπ emotet και trickbot, πληρωμές και στρατολόγηση μελών και τέλος κάποια ονόματα.

2020	2021	2022
36619 target	17383 defender	876 pumba
33114 bentley	9595 stern	795 tramp
18977 stern	7740 driver	692 mango
8952 deploy	5366 bio	490 cybergangster
7121 mushroom	5340 veron	432 demon
5991 professor	5225 hof	421 many
5939 hof	5190 mango	387 defender
5181 troy	3618 ttrr	313 bentley
4949 marsel	3386 skippy	288 skippy
4578 revers	3077 tramp	
4483 baget	3036 bentley	
4139 price		
4060 mors		
3812 dandis		
3808 strix		
3801 van		
3329 braun		
3155 kaktus		
2726 buza		
2628 defender		

Η εταιρία cyberint κατάφερε να καθορίσει ρόλους για πολλά από τα μέλη, κυρίως από το πλήθος, το περιεχόμενο και το ύφος των συζητήσεων μεταξύ τους. [26]

Cobaltstrike: Μια συνηθισμένη τεχνική του γκρουπ ήταν να χρησιμοποιεί το cobaltstrike. Στα αρχεία που διέρρευσαν βρέθηκαν τροποποιημένα εργαλεία και εγχειρίδιο γραμμένο στα Ρωσικά.



Xmrig: Μια άλλη διαρροή ήταν ένα τροποποιημένο Xmrig που περιείχε ένα κωδικοποιημένο πορτοφόλι, πιθανόν να ανήκει στο γκρουπ. Ο Xmrig είναι ένας Cpu/Gpu crypto miner ανοιχτού κώδικα, για νόμιμη χρήση εξόρυξης κρυπτονομισμάτων, που μπορεί να χρησιμοποιηθεί και για cryptojacking. Παρόλο που αυτή δεν είναι μια δραστηριότητα του γκρουπ, ίσως να ήταν μια μελλοντική προσπάθεια ή μια παράπλευρη δραστηριότητα κάποιων μελών, για να ενισχύσουν τα εισοδήματά τους.

Ransomware: Στην αρχή ο ερευνητής που ξεκίνησε την διαρροή δεν ήθελε να αποκαλύψει τον κώδικα, όμως έπειτα από λίγη πίεση το έκανε.

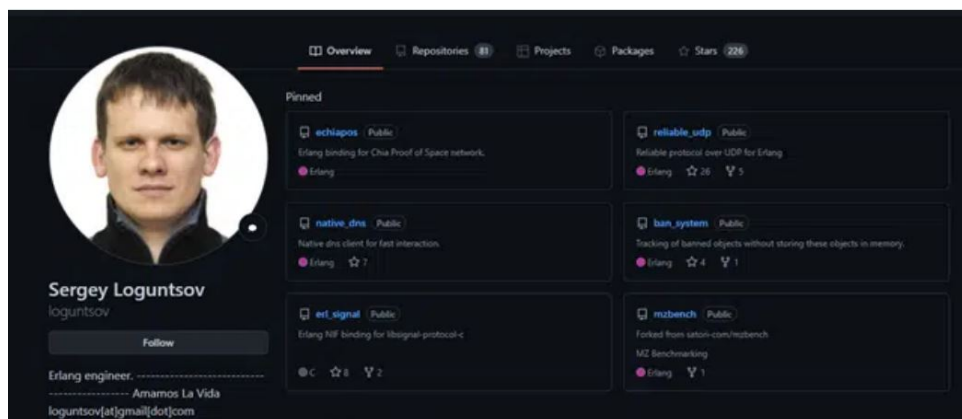


Φυσικά αποτελείται από δύο κύρια προγράμματα, τον locker και τον decryptor.

Ο Locker ακολουθεί την πεπατημένη, χρησιμοποιώντας γνωστούς αλγορίθμους κρυπτογράφησης, όπως chacha20 ενώ το κλειδί κρυπτογράφησης δημιουργείται δυναμικά.

Ο Decryptor είναι επίσης τυπικός και απλός. Το κυρίως πρόγραμμα περιέχει υποπρογράμματα που θα αναλάβουν τον έλεγχο του συστήματος αρχείων και του δικτύου που είναι προ απαιτούμενα για να προσπελάσει τα κρυπτογραφημένα αρχεία και να τα αποκρυπτογραφήσει.

Όσο παρουσιαζόταν νέα στοιχεία όμως, τόσο το γκρουπ προσαρμοζόταν στις νέες συνθήκες. Στην αρχή ακολούθησε μια τακτική ψυχραιμίας, δημοσιεύοντας μερικά νέα θύματα. Όταν είδαν όμως τις αντιδράσεις της κοινότητας, ειδικότερα των υπηρεσιών ασφάλειας οι οποίες πλέον ανέλυαν κάθε νέα πληροφορία και κάθε μήνυμα που ανταλλάχθηκε τα τελευταία δυο χρόνια, οι επικεφαλής προσπάθησαν να μειώσουν την ζημιά και να καλύψουν τα ίχνη τους, ειδικότερα αφού είδαν ότι κάποια μέλη αποκαλύφθηκαν πλήρως.



Οι τελευταίες συζητήσεις που διέρρευσαν δείχνουν ότι η απόφαση πάρθηκε να διαλυθεί ή να αποστασιοποιηθεί το γκρουπ για κάποιο διάστημα. Τα μέλη θα προσπαθούσαν να σβήσουν όλα τα αρχεία, να απενεργοποιήσουν όλα τα links που διέρρευσαν και να ρίξουν όλους τους servers τους. Επίσης σε κάποιες τελευταίες

συζητήσεις, τα μέλη του γκρουπ ψάχνουν ποιος έκανε την διαρροή και ποιος είναι ο Ουκρανός ερευνητής που παρουσιάζει τις πληροφορίες στο **conti leaks**. Εκεί φαίνεται να κυριαρχεί η άποψη ότι είναι κάποιο μέλος του γκρουπ το οποίο τους πρόδωσε. Σε κάθε περίπτωση τα μέλη θα προσπαθήσουν να ξαναφτιάξουν την υποδομή του γκρουπ και να επαναπροσδιορίσουν τους τρόπους επικοινωνίας τους, προσέχοντας να μην εκτεθούν επιπλέον στον Ουκρανό ερευνητή που τρέχει το **conti leaks**.

Ωστόσο η διαρροή του πηγαίου κώδικα και της ταυτότητας κάποιων μελών αποτελούν μεγάλη στιγμή στην ιστορία του ransomware, ειδικά αφού πρόκειται για ένα πολύ ενεργό γκρουπ, τόσο σε πλήθος επιθέσεων όσο και σε χρήμα που έχει προσποριστεί.

Κεφάλαιο Δ'

Συμπεράσματα

Η αγορά παράνομου λογισμικού στο dark web φαίνεται ότι είναι μια διαρκώς μεταβαλλόμενη αγορά, στην οποία πωλείται πλήθος κακόβουλων λογισμικών, κλεμμένων πληροφοριών και προσωπικά δεδομένα. Ακόμα κι όταν κάποιος βρει το προϊόν που επιθυμεί να αγοράσει, η επικοινωνία με τον πωλητή και η τελική αγορά του, εγκυμονεί κάποιους κινδύνους. Άλλοτε πάλι, οργανωμένες ομάδες πραγματοποιούν επιθέσεις με σκοπό τα λύτρα ή την κλοπή δεδομένων. Οι αρχές προσπαθούν πάντα να περιορίσουν τον ζωτικό χώρο για τους hackers, όμως διαρκώς βρίσκονται νέοι τρόποι επικοινωνίας και πωλήσεων. Το αποτέλεσμα είναι ότι τα οικονομικά μεγέθη της αγοράς αυτής διαρκώς μεγαλώνουν.

Δ.1 Τα κρυπτονομίσματα

Η αγορά κρυπτονομισμάτων γνωρίζει αρκετές διακυμάνσεις τα τελευταία χρόνια. Από την μια μεριά δημιουργούνται συνεχώς καινούρια κρυπτονομίσματα, με διαφορετικά χαρακτηριστικά ως προς την ασφάλεια και το όριο από τα προηγούμενα και από την άλλη οι τιμές των ήδη διαδεδομένων κρυπτονομισμάτων, όπως το bitcoin ή το ethereum αυξομειώνονται πολύ συχνά.

Ωστόσο η ανωνυμία που εξασφαλίζουν στον κάτοχό τους τα καθιστά ελκυστικά για αγορές όπου η ανωνυμία είναι βασική προτεραιότητα και ο χώρος του dark web είναι μια τέτοια περίπτωση. Είναι μονόδρομος λοιπόν η πώληση παράνομου λογισμικού, πληροφοριών και προσωπικών δεδομένων να γίνεται με κρυπτονομίσματα.

Τα πιο συχνά χρησιμοποιούμενα είναι το bitcoin, το monero, το ethereum. Παρόλο που το κόστος ενός προϊόντος δηλώνεται σε κάποιο τραπεζικό νόμισμα, συνήθως δολάρια, η πληρωμή πρέπει να γίνει με κάποιο κρυπτονόμισμα, με βάση την τρέχουσα ισοτιμία.

Δ.2 Επικοινωνία και πληρωμή του πωλητή

Η πληρωμή γίνεται σε κρυπτονομίσματα, συνήθως Bitcoin. Γίνεται προκαταβολικά αλλά σύμφωνα με τις ιστοσελίδες, αν ο πελάτης μετανιώσει σε σύντομο χρονικό διάστημα – συνήθως 4 ημέρες – μπορεί να ζητήσει ακύρωση της παραγγελίας και επιστροφή χρημάτων. Το ίδιο ισχύει αν δεν μείνει ευχαριστημένος από την υπηρεσία που του παρασχέθηκε, μπορεί να ζητήσει επιστροφή των χρημάτων του.

Αν κάποιος πελάτης είναι αρχάριος, μπορεί να ζητήσει οδηγίες για οτιδήποτε, όπως που να αγοράσει κρυπτονομίσματα ή πώς να ελέγξει το IMEI σε ένα κινητό τηλέφωνο. Ωστόσο υπάρχουν πάρα πολλά προβλήματα αξιοπιστίας και πολλές από αυτές τις σελίδες κλείνουν σύντομα, όταν αποδεικνύεται ότι πρόκειται για απατεώνες που απλά παίρνουν τα χρήματα των πελατών και εξαφανίζονται.

Πιο αξιόπιστες φαίνονται εκείνες οι σελίδες που είναι επιφυλακτικές απέναντι στον πελάτη. Σε αυτές ο πελάτης στέλνει ένα αίτημα σε μια διεύθυνση email και περιμένει να επικοινωνήσει κάποιος μαζί του. Αφού εξακριβωθούν οι προθέσεις του, του αποστέλλεται ένα ψηφιακό πορτοφόλι, στο οποίο πρέπει να καταθέσει το αντίτιμο σε Bitcoins. Αφού πληρώσει θα λάβει τον σύνδεσμο και τα στοιχεία σύνδεσης για το ιδιωτικό forum.

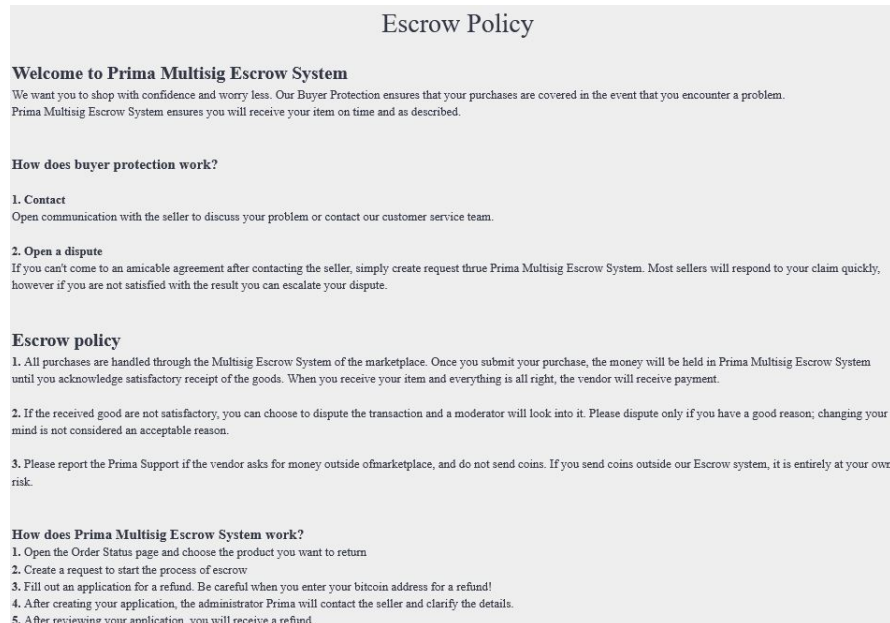
Το πρόβλημα της αξιοπιστίας υπάρχει και από τις δύο πλευρές, πράγμα αυτονόητο αφού οι υπηρεσίες που πωλούνται είναι παράνομες. Οι πωλητές απαιτούν προπληρωμή των υπηρεσιών τους, αφού ο πελάτης τους είναι άγνωστος και μπορεί να μην τους πληρώσει αν λάβει πρώτα το προϊόν ή την υπηρεσία που ζήτησε. Υπόσχονται ότι θα δώσουν κάποιες αποδείξεις της δουλειάς τους, πριν λάβουν την πληρωμή.

Από την άλλη πλευρά, οι πελάτες είναι επιφυλακτικοί επειδή και ο πωλητής είναι ανώνυμος οπότε φοβούνται ότι μπορεί να πέσουν θύματα απατεώνων. Οι απατεώνες αυτοί λειτουργούν συνήθως ως μεσάζοντες, φτιάχνοντας μια ψεύτικη ιστοσελίδα που πουλάει υπηρεσίες Hacking και περιμένοντας τα θύματα-πελάτες τους. Όταν τους δώσουν τα στοιχεία μιας «δουλειάς», όπως να παρακολουθήσουν ένα κινητό τηλέφωνο, αυτοί επικοινωνούν με κάποιον πραγματικό hacker στον οποίο δίνουν τα στοιχεία αυτά και απαιτούν μια πρώτη απόδειξη της ικανότητάς του να κάνει την δουλειά αυτή.

Όταν λάβουν από τον πραγματικό hacker την απόδειξη της ικανότητάς του να πραγματοποιήσει την δουλειά, η οποία μπορεί να είναι ένα αρχείο από τον υπολογιστή κάποιου ή μια φωτογραφία από το κινητό του, οι απατεώνες την προωθούν στο θύμα, δέχονται ολόκληρη την πληρωμή και φυσικά δεν κάνουν την δουλειά αλλά εξαφανίζονται, διακόπτοντας κάθε επικοινωνία.

Για τους παραπάνω λόγους, οι περισσότερες σελίδες του Dark web έχουν αναπτύξει τα τελευταία χρόνια ένα σύστημα εγγύησης πληρωμής (Escrow system) το οποίο εξασφαλίζει τον αγοραστή από πιθανή απάτη. Σε κάθε τέτοιο σύστημα, το οποίο η κάθε ιστοσελίδα διαφημίζει με το δικό της όνομα ως το πιο καλό και αξιόπιστο, ο αγοραστής καταθέτει το ποσό σε ένα εγγυητικό ταμείο και έτσι λαμβάνει το προϊόν ή την υπηρεσία που παρήγγειλε.

Αν μείνει ικανοποιημένος και ο πωλητής έχει καλύψει όλα τα επιμέρους στοιχεία της πώλησης, τότε δίνει μια επιβεβαίωση για αποδέσμευση του ποσού προς τον πωλητή. Αν δεν μείνει ευχαριστημένος τότε ζητά *ακύρωση της πληρωμής* (dispute), δίνοντας βέβαια έναν καλό λόγο ακύρωσης.



Εικόνα Δ 0.1 Σύστημα εγγύησης πληρωμής

Οι περισσότερες σελίδες προτρέπουν τους αγοραστές να χρησιμοποιούν το σύστημα εγγυημένης πληρωμής που διαθέτουν και να μην στέλνουν κρυπτονομίσματα απευθείας στον πωλητή. Τους ζητούν μάλιστα να αναφέρουν τέτοιες περιπτώσεις που κάποιος πωλητής ζητάει απευθείας πληρωμή.

Ένα σημαντικό μειονέκτημα του παραπάνω συστήματος είναι η εξασφάλιση της ανωνυμίας του αγοραστή, καθώς συνήθως ζητείται να έχει ένα λογαριασμό στην σελίδα και να έχει δώσει ένα ψηφιακό πορτοφόλι επιστροφής χρημάτων.

Δ.3 Τρόπος αποστολής

Η αποστολή των προϊόντων γίνεται μέσα από email, p2p ή αποθετήρια, όταν πρόκειται για προϊόντα λογισμικού. Έτσι είναι δυνατή η αποστολή του λογισμικού οπουδήποτε, ξεπερνώντας τους γεωγραφικούς περιορισμούς.

Σε περίπτωση υλικών αντικειμένων, όπως κλεμμένων πιστωτικών καρτών, πλαστών χαρτονομισμάτων ή διαβατηρίων, ο πωλητής υπόσχεται ότι η αποστολή θα γίνει διακριτικά, μέσω υπηρεσιών κούριερ σε οποιοδήποτε μέρος του κόσμου. Ωστόσο είναι προφανές ότι σε αυτή την περίπτωση, το ρίσκο είναι μεγαλύτερο για τον αγοραστή,

που θα δεχθεί το πακέτο, αφού πρέπει να δώσει κάποια πραγματική διεύθυνση αποστολής.

Η χρήση κρυπτονομισμάτων εξασφαλίζει την ανωνυμία των δύο πλευρών. Μετά την επιβεβαίωση της πληρωμής, ένα σύνδεσμος ενεργοποιείται ώστε να μπορέσει ο αγοραστής να παραλάβει το προϊόν που πλήρωσε. Τα πιο δημοφιλή παραμένουν τα bitcoin, monero, ethereum, ωστόσο με την διαρκή εξάπλωση τους και την δημιουργία νέων block chains, και άλλα κρυπτονομίσματα γίνονται αποδεκτά.

Κρυπτονομίσματα χρησιμοποιούνται και για λύτρα στις περιπτώσεις ransomware εναντίον ιδιωτών ή εταιριών. Στην δεύτερη περίπτωση τα ποσά είναι πολύ μεγάλα ώστε πρέπει άμεσα να διοχετευτούν σε πολλά μικρότερα πορτοφόλια, συνήθως σε διαφορετικά είδη κρυπτονομισμάτων. Ωστόσο είναι κοινή παραδοχή ότι αν πρέπει να μετατραπούν σε πραγματικό χρήμα, όπως ευρώ ή δολάρια, θα πρέπει πρώτα να επανέλθουν σε bitcoin πορτοφόλια, καθώς αυτό είναι το πιο διαδεδομένο νόμισμα που έχει την μεγαλύτερη ζήτηση.

Δ.4 Αξιοπιστία και εγγυήσεις σε ένα ανασφαλές περιβάλλον

Ένα σημαντικό θέμα είναι η αξιοπιστία των αγοραπωλησιών στο dark web. Σε μια εντελώς ανέλεγκτη αγορά, είναι συνηθισμένο φαινόμενο η παρουσία κάποιων «πονηρών» που θα προσπαθήσουν να εξαπατήσουν τους αγοραστές. Η παρουσία τους επηρεάζει και τους πωλητές βέβαια, καθώς πωλούν μη-λειτουργικό λογισμικό σε χαμηλότερες τιμές, τραβώντας έτσι την προσοχή των αγοραστών και στερώντας πελάτες από τους «τίμιους» πωλητές. Επίσης δημιουργούν ένα γενικότερο αίσθημα ανασφάλειας μεταξύ πωλητή-αγοραστή.

Τα τελευταία χρόνια γίνεται μια προσπάθεια για πιο «κλειστές» αγορές στο dark web, οι οποίες λειτουργούν με αυστηρούς κανόνες, ελέγχοντας τόσο τους πωλητές που δέχονται όσο και τους αγοραστές. Στις αγορές αυτές που λειτουργούν περισσότερο ως forums, γίνεται δεκτός κάποιος μόνο μετά από έλεγχο των διαχειριστών, έλεγχος που μπορεί να διαρκέσει και μήνες.

Ζητείται να δημιουργηθεί για αγοραστή ή πωλητή ένας λογαριασμός, ώστε να μπορεί να γίνει μια μόνιμη αξιολόγηση των υπηρεσιών που προσφέρονται (πωλητές) όσο και της συνέπειας στην πληρωμή (αγοραστές). Πολλές αρνητικές αξιολογήσεις μπορεί να οδηγήσουν κάποιον εκτός πλατφόρμας, όπως ακριβώς γίνεται και σε νόμιμες πλατφόρμες (e-bay, paypal)

Το ίδιο ισχύει και για πωλητές που έχουν πολλές ακυρώσεις παραγγελιών, για την ίδια ή διαφορετικές αιτίες. Όταν υπάρχουν ακυρώσεις μέσω του συστήματος εγγυημένης πληρωμής, η φήμη του πωλητή μειώνεται. Γι' αυτό και οι περισσότεροι πωλητές προτρέπουν τους πελάτες να επικοινωνήσουν μαζί τους πριν προβούν σε ακύρωση της παραγγελίας, ώστε να τους δοθεί η ευκαιρία να διορθώσουν την παραγγελία.

Βιβλιογραφία

- [1] «Wikipedia,» 2021. [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Dark_Web. [Πρόσβαση Οκτώβριος 2021].
- [2] P. H. Meland, Y. F. Fahmy Bayoumy και S. Guttom, «The Ransomware-as-a-Service economy within the darknet,» *Computers & Security*, p. 9, 29 2 2020.
- [3] «Καθημερινή,» 7 6 2021. [Ηλεκτρονικό]. Available: <https://www.kathimerini.gr/society/561390058/sta-adyta-toy-skoteinoy-diadiktyoy/>. [Πρόσβαση Οκτώβριος 2021].
- [4] «Kaspersky Labs,» 2021a. [Ηλεκτρονικό]. Available: <https://www.kaspersky.com/resource-center/threats/deep-web>. [Πρόσβαση 21 Νοέμβριος 2021].
- [5] P. Syverson, «Onion Routing,» 2015. [Ηλεκτρονικό]. Available: <https://www.onion-router.net/History.html>. [Πρόσβαση 21 Νοέμβριος 2021].
- [6] K. Swan, «Onion Routing and TOR,» *Georgetown Law Technology Review*, Georgetown , 2016.
- [7] «Comparitech Blog,» Comparitech, 2021. [Ηλεκτρονικό]. Available: <https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/>. [Πρόσβαση 23 10 2021].
- [8] «Tor project,» 2021. [Ηλεκτρονικό]. Available: <https://www.torproject.org/>. [Πρόσβαση 21 10 2021].
- [9] «Kaspersky Labs,» 21 Νοέμβριος 2021b. [Ηλεκτρονικό]. Available: <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>.
- [10] «Europol Media & Press,» 21 1 2022. [Ηλεκτρονικό]. Available: <https://www.europol.europa.eu/media-press/newsroom/news/unhappy-new-year-for-cybercriminals-vpnlabnet-goes-offline>. [Πρόσβαση 22 1 2022].
- [11] «Securelist by Kaspersky,» Kaspersky, 2021. [Ηλεκτρονικό]. Available: <https://securelist.com/kaspersky-security-bulletin-2020-2021-eu-statistics/102335/> . [Πρόσβαση 03 11 2021].
- [12] «AV test The independent IT-security institute,» AV test, 2022. [Ηλεκτρονικό]. Available: <https://www.av-test.org/en/statistics/malware/> . [Πρόσβαση 30 1 2022].
- [13] K. Finklea, «Dark Web,» *Congressional Research Service*, 2017.
- [14] «Cupertino Electric Inc. Blog,» Cupertino Electric, 2015. [Ηλεκτρονικό]. Available: <https://www.cei.com/about-cei/media-room/blog/cyber-security-targets-2013->

data-breach. [Πρόσβαση 19 11 2021].

- [15] J. Burgess, «Malware and Exploits on the Dark Web,» Queen's University Belfast, Belfast, 2017.
- [16] S. Morgan, «Cybercrime magazine,» 13 11 2020. [Ηλεκτρονικό]. Available: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>. [Πρόσβαση 12 11 2021].
- [17] M. Riek και R. Bohme, «The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates,» *Journal of Cybersecurity*, p. 16, 2018.
- [18] R. Anderson, C. Barton, R. Boehme, R. Clayton, C. Gannan, T. Grasso, M. Levi, T. Moore και M. Vasec, «Measuring the Changing Cost of Cybercrime,» *The 18th Annual Workshop on the Economics of Information Security*, τόμ. 1, αρ. 32, 2019.
- [19] «Securelist by Kaspersky,» Securelist, 2022. [Ηλεκτρονικό]. Available: <https://securelist.com/it-threat-evolution-in-q3-2021-pc-statistics/104982/>. [Πρόσβαση 4 2 2022].
- [20] J. Robertson, A. Diab, M. Ericsson, E. Nunes, V. Paliath, J. Shakarian και P. Shakarian, *Darkweb Cyber thread intelligence mining*, Cambridge University Press, 2017.
- [21] «Symantec Enterprise Blogs,» Broadcom software, 2020. [Ηλεκτρονικό]. Available: <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020>. [Πρόσβαση 23 11 2021].
- [22] K. A. Dwyer Katherine, «Gone in 200 milliseconds: the challenge of blocking malvertising,» *Pace Digital Repository*, p. 9, 2016.
- [23] «CrowdStrike services cyber front lines report,» CrowdStrike Inc, 2020. [Ηλεκτρονικό]. Available: <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf>. [Πρόσβαση 23 11 2021].
- [24] Secureworks, «2021 State of the Threat,» Secureworks, 2021.
- [25] C. Cabaluna, «Isaca,» 27 10 2021. [Ηλεκτρονικό]. Available: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-35/surge-in-ransomware-attack-and-10-biggest-attacks-in-2021>. [Πρόσβαση 4 2 2022].
- [26] S. Gihon, «Cyberint.com,» 2022. [Ηλεκτρονικό]. Available: <https://cyberint.com/blog/research/contileaks/>. [Πρόσβαση 24 03 2022].
- [27] R. Sion, *Hands-On Dark Web Analysis: Learn what goes on in the Dark Web, and how to work with it*, Packt Publishing, 2018.

- [28] H. Chen, «Dark Web: Exploring and Data Mining the Dark Side of the Web,» σε *International Conference on Formal Concept Analysis*, 2011.
- [29] S. Sagar, W. Li, V. Benjamin και H. Chen, «Informing Cyber Threat Intelligence through Dark Web Situational Awareness: The AZSecure Hacker Assets Portal,» *ACM Digital Library*, p. 10, 2021.
- [30] T. Holler, «Tor Blog,» 2021. [Ηλεκτρονικό]. Available: <https://blog.torproject.org/v3-onion-services-usage/>. [Πρόσβαση 21 11 2021].
- [31] B. Stone-Gross και P. Khandhar, «Secureworks Blog,» Secureworks, 17 12 2014. [Ηλεκτρονικό]. Available: <https://www.secureworks.com/research/dyre-banking-trojan>. [Πρόσβαση 8 12 2021].
- [32] S. Singh και Y. Wang, «Fireeye Blogs,» Fireeye, 7 7 2015. [Ηλεκτρονικό]. Available: https://www.fireeye.com/blog/threat-research/2015/07/dyre_banking_trojan.html. [Πρόσβαση 8 12 2021].
- [33] K. Christidis και M. Devetsikiotis, «Blockchains and Smart Contracts for the Internet of Things,» *IEEE Access*, p. 12, 10 5 2016.

[1]

Συντμήσεις

DDOS	Distributed Denial of Service
Malvertising	Malware advertising
VPN	Virtual Private Network
HSDir	Hidden Service Directory Κατάλογος κρυμμένων υπηρεσιών
KDF	Key Derivation Function
TOR	The Onion Routing
Ekit	Exploit kit
APT	Advanced Persistence Threat
AES	Advanced Encryption Standard
IDT	Identity Theft
EMPACT	European Multidisciplinary Platform Against Criminal Threats
PGP encryption	Pretty Good Privacy encryption
LEA	Law Enforcement Agency

Γλωσσάρι Ξενικών Όρων

Distributed Denial of Service	Κατανεμημένη επίθεση άρνησης υπηρεσιών
Malvertising	Προώθηση κακόβουλου λογισμικού μέσω διαφημίσεων
Vulnerability	Ευπάθεια προγράμματος / κενό ασφαλείας
Exploit kit / exploit pack	Τύπος κακόβουλου εργαλείου λογισμικού που προσπαθεί να εκμεταλλευτεί κενά ασφαλείας σε υπολογιστικά συστήματα ή δίκτυα υπολογιστών.
Initial access attack	Επίθεση αρχικής πρόσβασης, προσπάθεια πρόσβασης σε ένα υπολογιστικό σύστημα, ώστε να εγκατασταθεί κακόβουλο λογισμικό
Web Crawlers	Προγράμματα που διατρέχουν ιστοσελίδες και καταλογογραφούν το περιεχόμενό τους, με σκοπό την διευκόλυνση της αναζήτησης σε αυτές
Advanced Encryption Standard	Πρότυπο για την κρυπτογράφηση ηλεκτρονικών δεδομένων, το οποίο καθιερώθηκε το 2001.
Application layer	Επίπεδο εφαρμογής, ένα από τα 7 επίπεδα του μοντέλου OSI
Great Wall of China	Το μεγάλο τείχος προστασίας που προστατεύει το διαδίκτυο στην Κίνα
Dispute	Ακύρωση συναλλαγής
Escrow system	Σύστημα εγγύησης πληρωμής