Εισβολείς με ρόπαλα στα χέρια – Λεηλατούν σπίτια και χωράφια Ελλήνων – Εξοργιστικές εικόνες (ΒΙΝΤΕΟ)

Εισβολείς με ρόπαλα στα χέρια – Λεηλατούν σπίτια και χωράφια Ελλήνων – Εξοργιστικές εικόνες (ΒΙΝΤΕΟ)

Βρήκαν ευκαιρία με την καραντίνα – Σοκάρουν οι εικόνες από την Μόρια της Λέσβου… Ενώ οι Έλληνες βρίσκονται σε καραντίνα και περιορισμένη κυκλοφορία λόγω κορωνοϊού, οι μουσουλμάνοι εισβολείς λεηλατούν σπίτια, κόβουν δέντρα Ελλήνων και στην συνέχεια αθλούνται.05-04-2020-21:53

Βρήκαν ευκαιρία με την καραντίνα – Σοκάρουν οι εικόνες από την Μόρια της Λέσβου…

Ενώ οι Έλληνες βρίσκονται σε καραντίνα και περιορισμένη κυκλοφορία λόγω κορωνοϊού, οι μουσουλμάνοι εισβολείς λεηλατούν σπίτια, κόβουν δέντρα Ελλήνων και στην συνέχεια αθλούνται.

Μάλιστα βίντεο καταγράφει Αφγανούς μουσουλμάνους με ρόπαλα στα χέρια. Συγκεκριμένα μεγάλες ομάδες εισβολέων, κυρίως Αφγανικής υπηκοότητας κινήθηκαν με πέτρες και ρόπαλα στα χέρια, μέσα στα χωράφια, σε μια προσπάθεια να κινηθούν κατά άλλης ομάδας αλλοδαπών. Οι δυο ομάδες συνεπλάκησαν το απόγευμα της Τρίτης για άγνωστα κίνητρα.

Μάλιστα κατά τη διάρκεια της έντασης, διερχόμενο αυτοκίνητο με έναν επιβάτη δέχτηκε πέτρες με αποτέλεσμα όπως φαίνεται στις φωτογραφίες του lawandorder.gr να προκληθούν φθορές στο όχημα, ενώ από θαύμα δεν τραυματίστηκε σοβαρά ο οδηγός.

Το ίδιο συμβαίνει και σε άλλες περιοχές της Ελλάδας!

Δείτε:

Λεηλατούν σπίτια και χωράφια Ελλήνων

Λεηλατούν σπίτια και χωράφια Ελλήνων

Λεηλατούν σπίτια και χωράφια Ελλήνων

Λεηλατούν σπίτια και χωράφια Ελλήνων

Λεηλατούν σπίτια και χωράφια Ελλήνων

Λεηλατούν σπίτια και χωράφια Ελλήνων

Εισβολείς με ρόπαλα στα χέρια

ΚΟΙΝΟΠΟΙΗΣΕ ΠΑΝΤΟΥ – ΔΙΑΔΩΣΕ ΤΙΣ ΠΛΗΡΟΦΟΡΙΕΣ

ΣΕ ΣΧΟΛΙΑ Η ΑΝΑΡΤΗΣΕΙΣ ΑΛΛΩΝ BLOG Η SITES & ΣΕ ΔΙΑΦΟΡΕΤΙΚΕΣ ΟΜΑΔΕΣ facebook

ΠΗΓΗ:https://www.e-synews.gr/wp/2020/04/05/eisvoleis-ropala-sta-cheria-leilatoyn-spitia-chorafia/

Συνεχώς καταφθάνουν λεωφορεία με μετανάστες στο Σιδηρόκαστρο Σερρών – Κατά τα άλλα «Μένουμε σπίτι»

Συνεχώς καταφθάνουν λεωφορεία με μετανάστες στο Σιδηρόκαστρο Σερρών

Τα πρώτα λεωφορεία με παράνομους ξεκίνησαν να φτάνουν από τις 12 το μεσημέρι, στην περιοχή «Κλειδί», του Δήμου Σιντικής Σερρών, ενώ μέχρι νωρίς το μεσημέρι έφτασαν έξι λεωφορεία στον ειδικά διαμορφωμένο χώρο. Συνοδευόμενα από αστυνομική δύναμη, τα λεωφορεία μεταφέρονται από την Καβάλα, όπου κατέπλευσαν με καράβι που ξεκίνησε από τα νησιά.

Με το που έφτασαν οι παράνομοι μετανάστες στον ειδικά διαμορφωμένο χώρο, στην περιοχή «Κλειδί», έγινε η καταμέτρησή τους, στη συνέχεια υπεβλήθησαν σε ιατρικές εξετάσεις από κλιμάκιο του Ερυθρού Σταυρού για τυχόν ασθένειες και οδηγήθηκαν στις σκηνές τους.

Συνεχίζεται η ροή των λεωφορείων που μεταφέρουν μετανάστες στην κλειστή δομή των Σερρών, που βρίσκεται στη θέση «Κλειδί», σε μία από τις πλέον τουριστικές περιοχές, στο Ρούπελ του Δήμου Σιντικής.

Μέχρι αυτή την ώρα (13:24), σύμφωνα με το infonews24, έχουν φτάσει στην περιοχή έξι λεωφορεία, ενώ η ροή θα συνεχισθεί, καθώς στην κλειστή δομή αναμένεται θα φιλοξενηθούν 598 μετανάστες και έχουν τοποθετηθεί 60 σκηνές.

Το θέμα είναι ότι τη στιγμή που η ροή των μεταναστών συνεχίζεται, στο σημείο εξακολουθούν να δουλεύουν τα συνεργεία, καθώς οι εργασίες στην κλειστή δομή δεν έχουν ολοκληρωθεί.

Κατατέθηκαν οι ΠΝΠ για τις επιτάξεις

Κατατέθηκαν στη Βουλή προς κύρωση, όπως διαβάζουμε στο pronews, οι Πράξεις Νομοθετικού Περιεχομένου για την «επίταξη ακινήτων» σε νήσους υποδοχής μεταναστών και για την «αναστολή της υποβολής αιτήσεων χορήγησης ασύλου».

Συγκεκριμένα,

-κυρώνεται και αποκτά ισχύ νόμου από τότε που ίσχυσε, η από 10/02/2020 ΠΝΠ «Κατεπείγουσες «Κατεπείγουσες ρυθμίσεις επίταξης ακινήτων για την αποφυγή διακινδύνευσης της δημόσιας τάξης και υγείας» (Α’ 28), με την οποία προβλέπεται η επίταξη ακινήτων σε νήσους υποδοχής μεταναστών και προσφύγων των Περιφερειών Βορείου και Νοτίου Αιγαίου.**Δείτε επίσης:** Δάκρυσε ο Σ. Τσιόδρας όταν μίλησε για τους ηλικιωμένους, για τις μανάδες και τους πατεράδες μας

Για τα ακίνητα που ανήκουν σε ιδιώτες, ΟΤΑ και ΝΠΔΔ, καθορίζεται εύλογη αποζημίωση. Σημειώνεται ότι η προθεσμία έκδοσης της ΚΥΑ σχετικά με τον καθορισμό της αποζημίωσης των δικαιούχων, παρατείνεται για δύο μήνες, με δυνατότητα ισόχρονης παράτασης.

-κυρώνεται και αποκτά ισχύ νόμου από τότε που ίσχυσε, η από 02/03/2020 ΠΝΠ «Αναστολή της υποβολής αιτήσεων χορήγησης ασύλου» (Α’ 45), με την οποία αναστέλλεται, από την έναρξη ισχύος της κυρούμενης ΠΝΠ, η υποβολή των εν λόγω αιτήσεων, από άτομα που εισέρχονται στην χώρα παράνομα. Τα άτομα αυτά επιστρέφονται, χωρίς καταγραφή, στη χώρα προέλευσης ή καταγωγής. Η ρύθμιση ισχύει για ένα μήνα με δυνατότητα σύντμησης κατόπιν πράξης Υπουργικού Συμβουλίου.

Επίσης, απαλλάσσονται αναδρομικά από 24/02/2020 και για χρονικό διάστημα έξι μηνών από:

-τον ΦΠΑ, η ναύλωση και μίσθωση πλοίων ή αεροσκαφών που πραγματοποιούνται για τη μεταφορά ή φιλοξενία ή οποιαδήποτε άλλη χρήση με σκοπό την αντιμετώπιση των μεταναστευτικών ροών,

η παράδοση και η εισαγωγή καυσίμων, λιπαντικών, τροφοεφοδίων και λοιπών αγαθών, που προορίζονται για τον εφοδιασμό των πλοίων και αεροσκαφών αυτών.

-τον Ειδικό Φόρο Κατανάλωσης (ΕΦΚ) τα καύσιμα που προορίζονται για τις ανάγκες των δημοσίων αρχών,

-κάθε φόρο, τέλος, εισφορά ή κράτηση, η παράδοση ή εισαγωγή αγαθών καθώς και η παροχή υπηρεσιών για την αντιμετώπιση των μεταναστευτικών ροών ή έκτακτων και επειγουσών αναγκών.

ΠΗΓΗ:https://hellas-now.com/synechos-katafthanoyn-leoforeia-metanastes-sidirokastro-serron-ta-alla/?fbclid=IwAR13jj-gF4a6_7cxCn-L_fPHp3NS_gZ6JrNWMgq6GjGu0s2nHx_XXShbHTU

Κακοκαιρία – Δύο αρματαγωγά στη Σάμο για την προσωρινή φιλοξενία 1.000 ατόμων

Κακοκαιρία – Δύο αρματαγωγά στη Σάμο για την προσωρινή φιλοξενία 1.000 ατόμων

ΣΕ ΛΙΓΟ ΘΑ ΑΡΧΙΣΩ ΝΑ ΛΕΩ ΓΙΑ ΤΗΝ ΠΡΑΓΜΑΤΙΚΗ ΑΠΟΣΤΟΛΗ ΤΟΥ ΕΛΛΗΝΙΚΟΥ ΠΟΛΕΜΙΚΟΥ ΝΑΥΤΙΚΟΥ …. ΚΑΙ ΘΑ ΦΑΜΕ ΤΑ ΜΟΥΣΤΑΚΙΑ ΜΑΣ!!!!! ΕΝΑ ΘΑ ΠΩ….. ΣΥΝΘΗΚΗ ΤΗΣ ΓΕΝΕΥΗΣ….. Η ΕΠΟΙΚΙΣΗ ΕΙΝΑΙ ΕΚΓΛΗΜΑ ΠΟΛΕΜΟΥ ΚΑΙ ΔΙΩΚΕΤΑΙ!!!!! ΑΚΟΥΣ ΚΥΡΙΑΚΟΥΛΗ ΚΑΙ ΛΟΙΠΑ

ΕΡΠΕΤΑ ΚΑΙ ΠΤΗΝΑ ΤΟΥ ΔΑΣΟΥΣ;;;;; ΚΙ ΕΝΑ ΤΕΛΕΥΤΑΙΟ ….. ΑΥΤΑ ΤΑ ΠΛΗΡΩΝΟΥΜΕ ΕΜΕΙΣ!!! ΟΙ ΕΛΛΗΝΕΣ ΦΟΡΟΛΟΓΟΥΜΕΝΟΙ!!!!!

Patris Chatziantoniou

ΑΥΞΗΘΗΚΑΝ…….!

ΣΕ ΛΙΓΟ ΘΑ ΑΡΧΙΣΩ ΝΑ ΛΕΩ ΓΙΑ ΤΗΝ ΠΡΑΓΜΑΤΙΚΗ ΑΠΟΣΤΟΛΗ ΤΟΥ ΕΛΛΗΝΙΚΟΥ ΠΟΛΕΜΙΚΟΥ ΝΑΥΤΙΚΟΥ …. ΚΑΙ ΘΑ ΦΑΜΕ ΤΑ ΜΟΥΣΤΑΚΙΑ ΜΑΣ!!!!!

ΕΝΑ ΘΑ ΠΩ….. ΣΥΝΘΗΚΗ ΤΗΣ ΓΕΝΕΥΗΣ….. Η ΕΠΟΙΚΙΣΗ ΕΙΝΑΙ ΕΚΓΛΗΜΑ ΠΟΛΕΜΟΥ ΚΑΙ ΔΙΩΚΕΤΑΙ!!!!!

ΑΚΟΥΣ ΚΥΡΙΑΚΟΥΛΗ ΚΑΙ ΛΟΙΠΑ ΕΡΠΕΤΑ ΚΑΙ ΠΤΗΝΑ ΤΟΥ ΔΑΣΟΥΣ;;;;;

ΚΙ ΕΝΑ ΤΕΛΕΥΤΑΙΟ ….. ΑΥΤΑ ΤΑ ΠΛΗΡΩΝΟΥΜΕ ΕΜΕΙΣ!!! ΟΙ ΕΛΛΗΝΕΣ ΦΟΡΟΛΟΓΟΥΜΕΝΟΙ!!!!!

Τα αρματαγωγά θα παραμείνουν στο λιμάνι Μαλαγαρίου προληπτικά, λόγω της κακοκαιρίας που προβλέπει η ΕΜΥ στα νησιά του Βορείου Αιγαίου.

Αν υπάρξουν άσχημες καιρικές συνθήκες στη Σάμο και εφόσον δοθεί εντολή από την Πολιτική Προστασία, περίπου 1.000 (ΛΑΘΡΟ) πρόσφυγες και μετανάστες , κυρίως γυναικόπαιδα, ηλικιωμένοι και άλλα ευπαθή άτομα που διαμένουν στον καταυλισμό στο Βαθύ, θα μπορούν να φιλοξενηθούν προσωρινά στα πλοία, μέχρι να περάσει το κύμα κακοκαιρίας.

ΚΟΙΝΟΠΟΙΗΣΕ ΠΑΝΤΟΥ – ΔΙΑΔΩΣΕ ΤΙΣ ΠΛΗΡΟΦΟΡΙΕΣ

ΣΕ ΣΧΟΛΙΑ Η ΑΝΑΡΤΗΣΕΙΣ ΑΛΛΩΝ BLOG Η SITES & ΣΕ ΔΙΑΦΟΡΕΤΙΚΕΣ ΟΜΑΔΕΣ facebook

ΠΗΓΗ:https://www.e-synews.gr/wp/2020/01/05/kakokairia-dyo-armatagoga-sti-samo-tin-prosorini/

Ελληνικές εταιρείες θύματα του CrySIS/Dharma ransomware!

Μια επίθεση δίχως τέλος;

Ελληνικές εταιρείες θύματα του CrySIS/Dharma ransomware

Σύμφωνα με αρκετές αναφορές από μικρομεσαίες επιχειρήσεις αλλά και κολοσσούς στην Ελλάδα, το 2019 το CrySIS ή Dharma ransomware, το οποίο σπέρνει τον τρόμο στα θύματα τους από το 2016, έχει μολύνει αρκετές εταιρείες.

Ενώ η παγκόσμια online κοινότητα θεωρούσε ότι η τυραννία του CrySis ransomware είχε παρέλθει, **αρκετές ελληνικές επιχειρήσεις το διαψεύδουν πέφτοντας θύματα του malware** και πληρώνοντας -οι περισσότερες από αυτές- μεγάλα χρηματικά ποσά για την αποκρυπτογράφηση των αρχείων τους.

Μάλιστα, σύμφωνα με το Malwarebytes Labs, παρατηρείτε αύξηση των CrySIS ransomware επιθέσεων κατά 148% από τον Φεβρουάριο μέχρι τον Μάρτιο του 2019, σε παγκόσμιο επίπεδο.

Στον ελληνικό επιχειρηματικό κόσμο, το ransomware φαίνεται να έχει θορυβήσει αρκετές εταιρείες που θεωρούσαν τους

εαυτούς τους άτρωτους ή που δεν περίμεναν ποτέ να αποτελέσουν στόχο των hackers.

Μετά από έρευνα του SecNews, **οι hackers πίσω από τις επιθέσεις αποσκοπούν καθαρά στην αποκόμιση των χρηματικών ποσών** που ζητούν ως λύτρα. Αυτό σημαίνει ότι οι εταιρείες δεν αποτελούν στόχο προσωπικών συμφερόντων ή συνομωσιών από ανταγωνιστές τους.

Οι hackers λειτουργούν ως "επαγγελματίες" και μόλις λάβουν τα λύτρα αποστέλλουν το κλειδί αποκρυπτογράφησης των αρχείων.

Ελληνικές εταιρείες θύματα του CrySIS/Dharma ransomware

Σύμφωνα με την έρευνα του SecNews, πίσω από τις επιθέσεις

κρύβονται πιθανότατα, Κινέζικες ή/και Ρωσικές hacking ομάδες. Μάλιστα δε, πρόκειται για οργανωμένα groups τα οποία έχουν αποκομίσει ποσά τάξεως εκατομμυρίων (!) δολαρίων [σ.σ. 500.000.000$] από τις κακόβουλες ενέργειες.

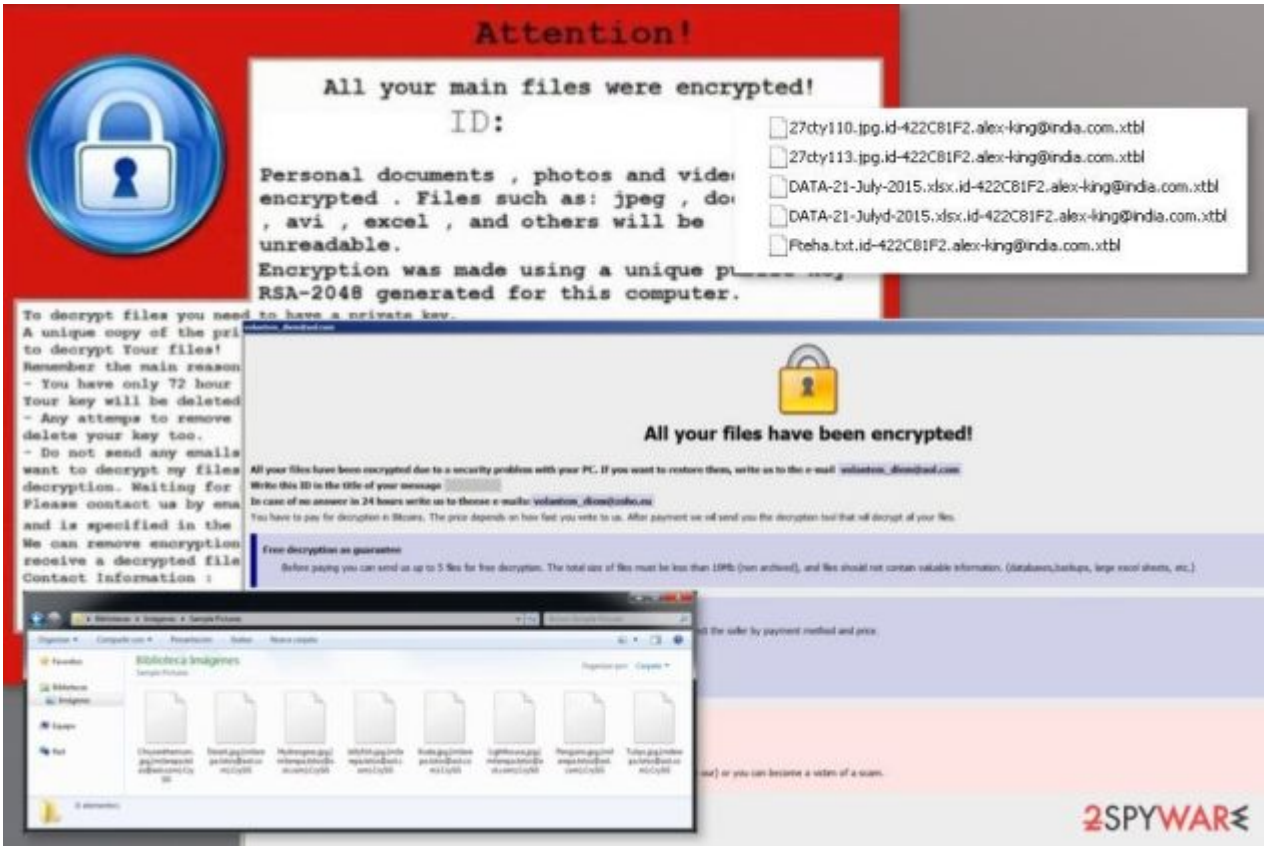
Τι είναι το CrySIS/Dharma ransomware και πως λειτουργεί;

Το CrySIS / Dharma στοχεύει Windows συστήματα, και απευθύνεται κυρίως σε επιχειρήσεις. Χρησιμοποιεί διάφορες μεθόδους διανομής:

- Το CrySIS διανέμεται ως **κακόβουλα συνημμένα σε spam emails**. Συγκεκριμένα, **τα κακόβουλα συνημμένα χρησιμοποιούν διπλές επεκτάσεις αρχείων, οι οποίες εντός default Windows settings ενδέχεται να φαίνονται μη εκτελέσιμες, ενώ στην πραγματικότητα είναι.**
- Το CrySIS μπορεί επίσης να καταλήξει **να μεταμφιεστεί ως αρχεία εγκατάστασης για νόμιμο λογισμικό,** συμπεριλαμβανομένων των AV vendors. Οι hackers πίσω από το CrySIS **προσφέρουν τους "άκακους" installers για διάφορες νόμιμες εφαρμογές ως εκτελέσιμα αρχεία που μπορούν να μεταφορτωθούν**, τα οποία έχουν διανεμηθεί μέσω διαφόρων τοποθεσιών στο διαδίκτυο και σε κοινόχρηστα δίκτυα.
- Τις περισσότερες φορές, το CrySIS / Dharma **παραδίδεται μη αυτόματα σε στοχευμένες επιθέσεις, εκμεταλλευόμενο διαπιστευτήρια RDP που έχουν διαρρεύσει ή είναι αδύναμα. Αυτό σημαίνει ότι ο επιτιθέμενος έχει πρόσβαση στα θύματα-μηχανές πριν από το brute-forcing attack σε Windows RDP protocol στη θύρα 3389.**

Σε μια πρόσφατη επίθεση, το CrySIS στάλθηκε ως download link σε ένα spam email. Ο σύνδεσμος κάνει redirect σε installer που προστατεύεται με κωδικό πρόσβασης. Ο κωδικός πρόσβασης δόθηκε στα δυνητικά θύματα στο ηλεκτρονικό ταχυδρομείο και εκτός από το εκτελέσιμο αρχείο CrySIS / Dharma, ο installer περιείχε ένα outdated εργαλείο αφαίρεσης από γνωστό προμηθευτή ασφάλειας.

Αυτή η social engineering στρατηγική χρησιμοποιήθηκε για να μην κινήσει υποψίες στους χρήστες. Βλέποντας μια οικεία λύση ασφάλειας στο πακέτο εγκατάστασης θεωρούν ότι το downloadable ήταν ασφαλές.



Ελληνικές εταιρείες θύματα του CrySIS/Dharma ransomware

Η μόλυνση

Μόλις το CrySIS μολύνει ένα σύστημα, **δημιουργεί registry entries και κρυπτογραφεί σχεδόν κάθε τύπο αρχείου**, παρακάμπτοντας τα αρχεία συστήματος και κακόβουλου λογισμικού. Εκτελεί την κρυπτογράφηση χρησιμοποιώντας έναν **ισχυρό αλγόριθμο κρυπτογράφησης** (AES-256 σε συνδυασμό με ασύμμετρη κρυπτογράφηση RSA-1024), **ο οποίος εφαρμόζεται σε σταθερούς, αφαιρούμενους και network δίσκους.**

Πριν από την κρυπτογράφηση, το CrySIS διαγράφει όλα τα Windows Restore Points εκτελώντας την εντολή vssadmin delete shadows / all / quiet.

Το Trojan που εξαπλώνεται εξαιτίας του ransomware **συλλέγει το όνομα του υπολογιστή** και **τον αριθμό κρυπτογραφημένων αρχείων από ορισμένες μορφές**, στέλνοντάς τα σε ένα απομακρυσμένο διακομιστή C2 που ελέγχεται από τον hacker. Σε ορισμένες Windows εκδόσεις, προσπαθεί επίσης να **δρα με δικαιώματα διαχειριστή**, επεκτείνοντας έτσι τη λίστα των αρχείων που μπορούν να κρυπτογραφηθούν.

Μετά από μια επιτυχημένη επίθεση με βάση το RDP, παρατηρήθηκε ότι πριν εκτελέσει το ωφέλιμο φορτίο ransomware, το CrySIS απεγκαθιστά το λογισμικό ασφαλείας που είναι εγκατεστημένο στο σύστημα.

Ελληνικές εταιρείες θύματα του CrySIS/Dharma ransomware

Το Ransom

Όταν το CrySIS ολοκληρώσει την κρυπτογράφηση, **αφήνει μια σημείωση στην επιφάνεια εργασίας με το ποσό που πρέπει να πληρώσει το θύμα** αν επιθυμεί να λάβει πίσω τα αρχεία του, παρέχοντας δύο διευθύνσεις ηλεκτρονικού ταχυδρομείου για την επικοινωνία με τους hackers.

Τα απαιτούμενα λύτρα είναι συνήθως περίπου 1 Bitcoin, αλλά υπήρξαν περιπτώσεις όπου **η τιμολόγηση φαίνεται να έχει προσαρμοστεί ανάλογα με τα έσοδα της επηρεαζόμενης εταιρείας. Οι οικονομικά υγιείς εταιρείες συχνά πληρώνουν μεγαλύτερο ποσό.**

Πως να προστατευτείτε;

Παρόλο που έχετε την επιλογή να χρησιμοποιήσετε άλλο λογισμικό για να λειτουργήσετε εξ αποστάσεως τους υπολογιστές εργασίας σας, το RDP είναι ουσιαστικά ένα ασφαλές και εύκολο στη χρήση πρωτόκολλο με προεγκατεστημένο client σε συστήματα Windows, καθώς και clients που είναι διαθέσιμοι για άλλα λειτουργικά συστήματα. **Υπάρχουν μερικά μέτρα που μπορείτε να πάρετε για να καταστεί πολύ πιο δύσκολο να αποκτήσει κάποιος πρόσβαση στο δίκτυό σας μέσω μη εξουσιοδοτημένων συνδέσεων RDP:**

- Για να καταστεί πιο δύσκολο για μια brute force επίθεση να επιτύχει, **χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης.**

- **Μην απενεργοποιείτε** τον έλεγχο ταυτότητας επιπέδου δικτύου **(Network Level Authentication – NLA)** καθώς προσφέρει ένα επιπλέον επίπεδο ελέγχου ταυτότητας. Ενεργοποιήστε το αν δεν ήταν ήδη.

- **Αλλάξτε τη θύρα RDP** έτσι ώστε οι port-scanners που αναζητούν ανοιχτές θύρες RDP να χάσουν τη δική σας. Από προεπιλογή, ο διακομιστής **ακούει στη θύρα 3389** τόσο για TCP όσο και για UDP.

- Ή **χρησιμοποιήστε έναν απομακρυσμένο διακομιστή Gateway Server**, ο οποίος σας δίνει επίσης μερικά πρόσθετα πλεονεκτήματα ασφάλειας και λειτουργίας όπως το 2FA. **Τα logs των RDP sessions** μπορούν να αποδειχθούν ιδιαίτερα χρήσιμα όταν επιθυμείτε να ελέγξετε τις διάφορες κινήσεις. Καθώς αυτά τα logs δεν βρίσκονται στο παραβιασμένο μηχάνημα, είναι πιο δύσκολο να παραποιηθούν από hackers.

- **Περιορίστε την πρόσβαση σε συγκεκριμένες διευθύνσεις IP**,

εάν είναι εφικτό. Δεν θα πρέπει να υπάρχει ανάγκη για πολλές IPs που χρειάζονται πρόσβαση στο RDP.

- Υπάρχουν πολλές δυνατότητες αύξησης των δικαιωμάτων των χρηστών σε υπολογιστές Windows, ακόμα και όταν χρησιμοποιείτε RDP, αλλά όλες οι γνωστές μέθοδοι έχουν τροποποιηθεί (patched). **Έτσι, όπως πάντα, σιγουρευτείτε ότι τα συστήματά σας είναι πλήρως ενημερωμένα και patched.**

- Χρησιμοποιήστε μια αποτελεσματική και εύχρηστη **στρατηγική δημιουργίας αντιγράφων ασφαλείας.** Η εμπιστοσύνη στα Restore Points δεν πληροί τις προϋποθέσεις και είναι τελείως άχρηστη όταν το ransomware διαγράψει πρώτα τα σημεία επαναφοράς, όπως συμβαίνει στην περίπτωση του CrySIS.

- **Εκπαιδεύστε το προσωπικό** σας σχετικά με τις phishing επιθέσεις και ενισχύστε την ευαισθητοποίηση του αναφορικά με το cyber security.

- Τέλος, **χρησιμοποιήστε μια πολυεπίπεδη, προηγμένη λύση ασφάλειας** για την προστασία των μηχανών σας από επιθέσεις ransomware.

Ελληνικές εταιρείες θύματα του CrySIS/Dharma ransomware

IOCsΤο Ransom.Crysis είναι γνωστό ότι χρησιμοποιεί αυτές τις επεκτάσεις για κρυπτογραφημένα αρχεία:.crysis, .dharma, wallet, .java, .adobe, .viper1, .write, .bip, .zzzzz, .viper2, .arrow, .gif, .xtbl, .onion, .bip, .cezar, .combo, .cesar, .cmb, .AUF, .arena, .brrr, .btc, .cobra, .gamma, .heets, .java, .monro, .USA, .bkp, .xwx, .btc, .best, .bgtx, .boost, .heets, .waifu, .qwe, .gamma, .ETH, .bet, ta, .air, .vanss, .888, .FUNNY, .amber, .gdb, .frend, .like, .KARLS, .xxxxx, .aqva, .lock, .korea, .plomb, .tron, .NWA, .AUDIT, .com, .cccmn, .azero, .Bear, .bk666, .fire, .stun, .myjob, .ms13, .war, .carcn, .risk, .btix, .bkpx, .he, .ets, .santa, .gate, .bizer, .LOVE, .LDPR, .MERS, .bat, .qbix, .aa1, and .walΜέχρι στιγμής, έχουν εντοπιστεί τα ακόλουθα ransom ονόματα:

- txt
- HOW TO DECRYPT YOUR DATA.txt

- Readme to restore your files.txt
- Decryption instructions.txt
- FILES ENCRYPTED.txt
- Files encrypted!!.txt

htaΣυνηθισμένα file hashes:

- 0aaad9fd6d9de6a189e89709e052f06b
- bd3e58a09341d6f40bf9178940ef6603
- 38dd369ddf045d1b9e1bfbb15a463d4c

Σε περίπτωση που έχετε πέσει θύμα της συγκεκριμένης επίθεσης μπορείτε να επικοινωνήσετε με την ερευνητική ομάδα του SecNews κάνοντας κλικ στο https://www.secnews.gr/ask-us/*.Για λόγους απορρήτου τα ονόματα των ελληνικών εταιρειών που έχουν πέσει θύματα του CrySIS/Dharma ramsomware, δεν αποκαλύπτονται.*

ΚΟΙΝΟΠΟΙΗΣΕ ΠΑΝΤΟΥ – ΔΙΑΔΩΣΕ ΤΙΣ ΠΛΗΡΟΦΟΡΙΕΣ

ΣΕ ΣΧΟΛΙΑ Η ΑΝΑΡΤΗΣΕΙΣ ΑΛΛΩΝ BLOG Η SITES & ΣΕ ΔΙΑΦΟΡΕΤΙΚΕΣ ΟΜΑΔΕΣ facebook

ΠΗΓΗ:https://www.e-synews.gr/wp/2020/01/04/ellinikes-etaireies-thymata-crysis-dharma-ransomware-mia-epithesi/