RANSOMWARE

Επιμολύνσεις – Λύσεις - Αποτροπή

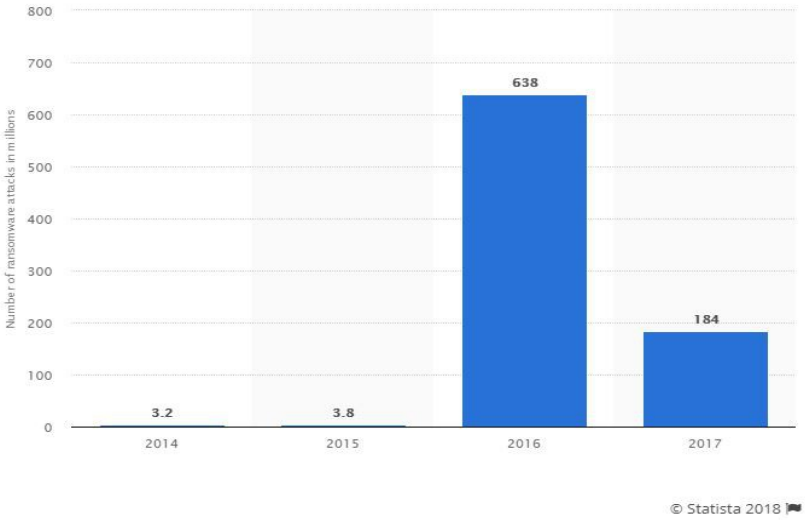
www.northwind.gr

ΓΕΝΙΚΑ

Οι Ransomware αποτελούν την λαίλαπα των τελευταίων ετών σε ό,τι αφορά την επιμόλυνση κάθε τύπου αποθηκευτικού μέσου και Η/Υ με κακόβουλο λογισμικό.

Μερικά στατιστικά στοιχεία:

- Το 70% των επιχειρήσεων πλήρωσαν τα λύτρα προκειμένου να πάρουν πίσω τα δεδομένα τους, την τριετία 2015-2018. Μόλις το 50% αυτών, τα πήρε.



Επιμολύνσεις από Ransomware παγκοσμίως, σε εκατομμύρια

- Το Ransomware κοστίζει στις επιχειρήσεις περισσότερα από 75 δισεκατομμύρια δολλάρια ανά έτος.
- Για την τριετία 2015-2018, οι επιχειρήσεις πλήρωσαν περίπου 900 δισεκατομμύρια δολλάρια για λύτρα.
- Τα απαιτούμενα λύτρα σε περίπτωση επιμόλυνσης είναι της τάξης των $500-$3000. Ένα 10% των θυμάτων ανέφερε ότι τα ζητούμενα λύτρα ήταν της τάξης των $5000 ή και περισσότερα.
- 25% των ερωτηθέντων δήλωσαν ότι θα πλήρωναν ένα ποσό της τάξης των $20.000-$50.000 σε περίπτωση επιμόλυνσης.
- Η Fedex δήλωσε ότι λόγω της επιμόλυνσης με τον NotPetya είχε απώλειες της τάξης των $300 εκατομμυρίων για το πρώτο τετράμηνο του 2017.
- Η παγκόσμια ζημιά στις επιχειρήσεις λόγω του NotPetya αγγίζει το 1 δισεκατομμύριο δολλάρια.
- Μετά την επίθεση που υπέστη η πόλη της Ατλάντα στην Georgia των ΗΠΑ από τον SamSam Ransomware τον Μάρτιο του 2018, αναφέρεται ότι χρειάστηκε να ξοδευτεί

το ποσό των 5 εκατομμυρίων δολλαρίων προκειμένου να ξαναστηθεί η υποδομή των δικτών της πόλης.

Πηγές: Dotto, IBM, Kaspersky, Malwarebytes, StateScoop, eWeek, Symantec.

Τα πρώτα κρούσματα εμφανίστηκαν το 2013, όταν ο διαβόητος Cryptolocker επιτέθηκε στα πρώτα του θύματα. Έκτοτε, ο τρόπος επίθεσης, ο τρόπος επιμόλυνσης αλλά και η επιλογή των θυμάτων έχει αλλάξει άρδην.

Πλέον, οι επιθέσεις είναι πιο στοχευμένες και λιγότερο στα "τυφλά".
Παρατηρούνται λιγότερα νέα στελέχη σε σχέση με τα προηγούμενα χρόνια, όμως ο αριθμός των παραλλαγών των υπαρχόντων στελεχών τριπλασιάστηκε μέσα στο 2018. Αυτό οφείλεται στο γεγονός ότι τα περισσότερα από τα υπάρχοντα στελέχη είναι δοκιμασμένα στο χρόνο και στις ευπάθειες, επομένως οι κακοποιοί απλώς ακολοθούν μία ήδη δοκιμασμένη συνταγή.

Στην **Ελλάδα**, έχουμε παρατηρήσει έξαρση του φαινομένου των επιμολύνσεων με Ransomware τα τελευταία χρόνια.
Ειδικότερα, για την διετία 2017-2018 οι αναφορές σε επιμολύνσεις αναφέρουν ιδιαίτερη έξαρση (με σειρά σημαντικότητας) στους Dharma, Locky, Cryptolocker, GandCrab, Scarab, GlobeImposter, Nemucod, Xorist αλλά και αρκετά ακόμα, μικρότερα στελέχη.

Σε κάποιες από αυτές τις περιπτώσεις ήταν δυνατή η αποκρυπτογράφηση των δεδομένων, ενώ σε κάποιες άλλες δυστυχώς δεν υπήρχε πλήρης λύση.

ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ RANSOMWARE

Ο τρόπος λειτουργίας τους είναι λίγο - πολύ ο ίδιος:
Ο υπολογιστής μολύνεται με το Ransomware (συνήθως από κάποιο παραπλανητικό email που ζητάει να γίνει click σε κάποιο link ή από επίσκεψη σε ιστοσελίδες αμφιβόλου ποιότητας ή από εκτεθειμένες υπηρεσίες απομακρυσμένης πρόσβασης -Remote Desktop- οι οποίες δεν βρίσκονται πίσω από κάποιο VPN), το οποίο κρυπτογραφεί τα δεδομένα με **AES256** κρυπτογράφηση και στέλνει το κλειδί στον επιτιθέμενο.
Το αποτέλεσμα είναι τα αρχεία να γίνονται μη-λειτουργικά, με περίεργες επεκτάσεις (πχ. Scan001.cezar ή σε γενικές γραμμές scan001.jpg.[επέκταση]) και είναι αδύνατον να χρησιμοποιηθούν.

Στη συνέχεια το κακόβουλο λογισμικό δημιουργεί μια αρχική οθόνη στην οποία ο χρήστης ενημερώνεται για το γεγονός ότι τα δεδομένα του δίσκου έχουν **κρυπτογραφηθεί** και ζητείται να καταβληθούν λύτρα έτσι ώστε να τους δοθεί το κλειδί για την

αποκρυπτογράφηση των δεδομένων. Συνήθως τα λύτρα καταβάλλονται μέσω bitcoin και η όλη διαδικασία γίνεται μέσω Tor για να μην είναι δυνατός ο εντοπισμός των δραστών.

Αξίζει να σημειωθεί πως ακόμα και αν καταβληθεί το ποσό που ζητείται, δεν υπάρχει καμία εγγύηση ότι οι δράστες θα παραχωρήσουν το κλειδί για την αποκρυπτογράφηση και αυτό είναι ευκόλως εννοούμενο, αφού στην πραγματικότητα η πληρωμή γίνεται προς κακοποιά στοιχεία τα οποία αναζητά το FBI.

Επίσης αξίζει να σημειωθεί πως η αρχική έκδοση του στελέχους αυτού, στόχευε μόνο Windows Servers (και κυρίως τις εκδόσεις 2003 και νωρίτερες), οι οποίοι είχαν ενεργοποιημένο το ενσωματωμένο Remote Desktop των Windows στην default port (3389). Οι δράστες αξιοποιούσαν ένα κενό ασφαλείας της συγκεκριμένης εφαρμογής, εγκαθιστούσαν τον εν λόγω Ransomware στον δίσκο, κρυπτογραφούσαν τα δεδομένα με τη δημιουργία ενός random κλειδιού 128bit το οποίο έστελναν στον εαυτό τους και στη συνέχεια το διέγραφαν από τον τοπικό δίσκο με sdelete έτσι ώστε να μην είναι δυνατή η ανάκτηση του ίχνους του.
Στη συνέχεια το στέλεχος εξελίχθηκε με **256bit** κρυπτογράφηση και με μη-αποθήκευση του κλειδιού τοπικά έτσι ώστε να είναι αδύνατη η αποκρυπτογράφηση των δεδομένων.
Αυτή η μέθοδος είναι πλέον η πιο διαδεδομένη, καθώς είναι στοχευμένη προς μεγάλες εταιρίες και οργανισμούς. Στις περιπτώσεις αυτές, τα ζητούμενα λύτρα ανέρχονται σε αρκετές δεκάδες χιλιάδων ευρώ.

Θα πρέπει επίσης να τονίσουμε πως οι Ransomware στοχεύουν συνήθως σε όλους τους τοπικούς δίσκους του υπολογιστή, καθώς και σε όλους τους εξωτερικούς που είναι συνδεδεμένοι αλλά και στους δικτυακούς δίσκους. Γενικά, χτυπάει όλους **τους δίσκους που έχουν γράμμα δίσκου** (C:, D:, X: κλπ), ενώ κάποια πιο εξελιγμένα στελέχη εντοπίζουν και συνδέονται ακόμα και σε δίσκους που δεν έχουν γίνει map και επομένως δεν τους έχει αντιστοιχιστεί γράμμα δίσκου.

Πως λειτουργούν οι Ransom/Crypto Ιοί:

1. Ο υπολογιστής μολύνεται από άνοιγμα links ή επισυναπτόμενων των email ή μέσω ιστοσελίδων. Το malware εγκαθίσταται στον υπολογιστή που δέχεται την επίθεση. Δεν ζητείται η συγκατάθεση του χρήστη.
2. Το κακόβουλο λογισμικό επικοινωνεί με τον server του επιτιθέμενου και ζητάει ένα public RSA κλειδί. Το public RSA κλειδί μπορεί να κρυπτογραφήσει αλλά όχι να αποκρυπτογραφήσει.
3. Στη συνέχεια δημιουργεί ένα AES κλειδί (μερικές φορές δημιουργεί ένα κλειδί για κάθε αρχείο) και κρυπτογραφεί το αρχείο χρησιμοποιώντας AES κρυπτογράφηση. Το πρωτότυπο αρχείο στη συνέχεια διαγράφεται.
4. Το AES κλειδί κρυπτογραφείται με το Public RSA κλειδί και αποθηκεύεται σε κάποιο σημείο του κρυπτογραφημένου αντιγράφου του πρωτότυπου αρχείου.
5. Ενημερώνεται το θύμα για το συμβάν και ζητούνται λύτρα για την αποκρυπτογράφηση.

ΕΝΑΛΛΑΚΤΙΚΑ,

1. Ο επιτιθέμενος εντοπίζει εκτεθειμένες υπηρεσίες Remote Desktop στον Η/Υ του θύματός του χρησιμοποιώντας εξειδικευμένα bots ή χτυπώντας στοχευμένα.
2. Χρησιμοποιείται η μέθοδος του Brute Force για να αποκτηθεί πρόσβαση στον Η/Υ του θύματος, και μόλις αυτό επιτευχθεί, εγκαθιστά χειροκίνητα το κακόβουλο λογισμικό, το οποίο εν συνεχεία κάνει ανενόχλητο τη δουλειά του, ενώ ο χρήστης στην πλειοψηφία των περιπτώσεων δεν αντιλαμβάνεται το παραμικρό.
3. Μόλις ολοκληρωθεί η επιμόλυνση, ακολουθούνται τα 2-5 της προηγούμενης περίπτωσης.

DHARMA RANSOMWARE

Ο Dharma αποτελεί έναν από τους πιο sophisticated Ransomware που κυκλοφόρησαν ποτέ. Με πολύ έντονη δραστηριότητα από τα πρώτα χρόνια εξάπλωσης των Ransomware (2015), η πρώτη του έκδοση διασπείρονταν αποκλειστικά μέσω email και τοποθετούσε την επέκταση .dharma στα κρυπτογραφημένα αρχεία. "Κάποιος" δημοσίευσε σε public forum το master key για τον Dharma v.1 και τον Μάρτιο του 2017 η Kaspersky κυκλοφόρησε τον αντίστοιχο decryptor.

Ακολούθησαν οι περιβόητες εκδόσεις .wallet και .onion οι οποίες προκάλεσαν χάος σε όλο τον κόσμο, κυρίως λόγω του εξαιρετικά αποτελεσματικού τρόπου διασποράς τους.
Σε αντίθεση με τους υπόλοιπους "διάσημους" Ransomware (όπως πχ. ο Locky), ο Dharma από το ξεκίνημά του μέχρι και σήμερα διασπείρεται με στοχευμένες επιθέσεις μέσω των υπηρεσιών απομακρυσμένης πρόσβασης (Remote Desktop Services – RDS). Με τη μέθοδο του Brute Force "σπάνε" αδύναμους κωδικούς στο RDS και εγκαθιστούν τον Ransomware.


Grizzly@airmail.cc

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail Grizzly@airmail.cc
Write this ID in the title of your message
In case of no answer in 24 hours write us to theese e-mails: Grizzlymail@qq.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Το Ransom Note του Dharma

Τον Μάιο του 2017 "κάποιος" άλλος δημοσιοποίησε το master key και για αυτές τις δύο εκδόσεις, κάνοντας πολύ κόσμο χαρούμενο.

Δυστυχώς η χαρά δεν κράτησε πολύ, καθώς την επόμενη κιόλας μέρα, κυκλοφόρησε νέα έκδοση του Dharma η οποία παραμένει απαραβιάστη μέχρι και σήμερα. Έκτοτε, έχουνε κυκλοφορήσει δεκάδες παραλλαγές του (.bip, .arena, .cezar, .brr, .cmb, .XXXXX και δεκάδες άλλα), χωρίς δυστυχώς να υπάρχει λύση για καμία από αυτές.

Ο Dharma από το ξεκίνημά του ήταν απαραβίαστος. Δεν έχει ευπάθειες που να μπορούμε να εκμεταλλευτούμε προκειμένου να τον αποκρυπτογραφήσουμε.
Τον τελευταίο καιρό έχουν κάνει μάλιστα την εμφάνισή τους διάφοροι επιτήδειοι οι οποίοι ισχυρίζονται ότι έχουν λύση για τον Dharma και ζητούν 3000-6000 ευρώ για την αποκρυπτογράφηση (περισσότερο από όσο ζητάει ο ίδιος ο Dharma, δηλαδή).
Πρόκειται για απατεώνες, που έχουν έρθει σε συμφωνία με τους δημιουργούς του κακόβουλου λογισμικού, και παίρνουν προμήθεια για κάθε "πώληση" που κάνουν.
ΔΕΝ ΥΠΑΡΧΕΙ ΠΕΡΙΠΤΩΣΗ ΝΑ "ΣΠΑΣΕΙ" Ο DHARMA ΧΩΡΙΣ ΤΟ MASTER ΚΛΕΙΔΙ.

Κρούσματα στην Ελλάδα

Έχουν αναφερθεί εκατοντάδες θύματα του Dharma και στην Ελλάδα.
Σύμφωνα με έρευνα της Northwind Data Recovery:
Ένα 8% δηλώνει ότι δεν πλήρωσε τα λύτρα και έχασε τα δεδομένα του
Ένα 19.6% δηλώνει ότι πλήρωσε τα λύτρα αλλά δεν πήρε ποτέ δεδομένα
Ένα 53.3% δηλώνει ότι δεν πλήρωσε τα λύτρα καθώς είχε αντίγραφα ασφαλείας
και ένα 19.1% δήλωσε ότι πλήρωσε τα λύτρα και πήρε δεδομένα.

Τα νούμερα αυτά συνοψίζονται στα συμπεράσματα ότι
Α) Οι μισοί χρήστες δεν τηρούν αντίγραφα
Β) Το 40% των θυμάτων αποφάσισε να πληρώσει τους εγκληματίες και
Γ) Οι μισοί από αυτούς δεν πήραν ποτέ πίσω τα δεδομένα τους.

Τρόποι αντιμετώπισης

Όπως προαναφέραμε, δεν υπάρχει τρόπος αποκρυπτογράφησης του Dharma. Ο μόνος τρόπος αντιμετώπισης είναι η πρόληψη.

Για το λόγο αυτό, η Northwind Data Recovery έχει συντάξει έναν οδηγό επιβίωσης τον οποίο θα πρέπει όλοι να ακολουθούν προκειμένου να μείνουν μακριά από επιμολύνσεις Ransomware.
Τον οδηγό μπορείτε να τον βρείτε στο blog της εταιρίας.

ΛΥΣΕΙΣ ΓΙΑ ΤΟΥΣ RANSOMWARE

Λύση με την έννοια της αποκρυπτογράφησης των δεδομένων που έχουν επιμολυνθεί/κρυπτογραφηθεί από Ransomware, εννοούμε τον εντοπισμό και εκμετάλλευση κάποιας ευπάθειας στον τρόπο με τον οποίο λειτουργεί το εν λόγω στέλεχος, με χρήση τεχνικών Reverse Engineering.

Τέτοιου είδους λύσεις έχουμε εφαρμόσει σε περιστατικά όπου οι μηχανικοί μας ανακάλυψαν ευπάθειες σε διάφορα στελέχη, με σημαντικότερες τις περιπτώσεις των

- Cryptolocker
- Scarab

όπου εντοπίσαμε ευπάθειες και καταφέραμε να αποκρυπτογραφήσουμε πλήρως εκατοντάδες περιστατικά επιμολύνσεων με τα εν λόγω στελέχη σε όλο τον κόσμο.

Ακόμα και στις περιπτώσεις όπου το στέλεχος δεν παρουσιάζει αδυναμίες και επομένως η εξεύρεση λύσεις με RE είναι αδύνατη, τότε υπό προϋποθέσεις, υπάρχει πιθανότητα να ανακτηθούν δεδομένα αν εξακολουθεί να υπάρχει πρόσβαση στον αρχικά μολυσμένο δίσκο και εκείνος δεν έχει τροποποιηθεί με κάποιον τρόπο. Στην περίπτωση αυτή, η λύση δεν είναι πλήρης, όμως έχουμε εντυπωσιακά αποτελέσματα ακόμα και τότε.

ΟΔΗΓΟΣ ΕΠΙΒΙΩΣΗΣ ΕΝΑΝΤΙΑ ΣΤΟΥΣ RANSOMWARE

Ας ξεκινήσουμε από τα βασικά:

Οι Ransomware είναι κακόβουλα λογισμικά τα οποία επιτίθενται και κρυπτογραφούν τα δεδομένα του θύματός τους, ενώ στη συνέχεια ζητούν την πληρωμή λύτρων με μορφή Bitcoin για την αποκρυπτογράφηση.

Με την έξαρση που παρουσιάζουν οι επιμολύνσεις από τους Ransomware τα τελευταία χρόνια, ακόμα και οι πιο έμπειροι χρήστες μπορεί να την πατήσουν, πόσο μάλλον οι λιγότερο εξοικιωμένοι.

Στη Northwind Data Recovery, χρησιμοποιούμε όλες τις διαθέσιμες τεχνικές για να μπορέσουμε να αποκρυπτογραφήσουμε τα δεδομένα που έχουν επιμολυνθεί, όμως κάποιες φορές ερχόμαστε στη δυσάρεστη θέση να ενημερώσουμε τους πελάτες μας ότι ούτε κι εμείς πλέον μπορούμε να κάνουμε κάτι για να τους βοηθήσουμε.

Για να μην έρθουμε λοιπόν σε αυτή τη δυσάρεστη θέση, ετοιμάσαμε έναν οδηγό για να βοηθήσουμε όλους τους ενδιαφερόμενους να αποφύγουν τις επιθέσεις των Ransomware. Ακολουθώντας αυτά τα βήματα, θα μπορείτε να θωρακίσετε τον Η/Υ σας και κατ' επέκταση τον εαυτό σας, τα δεδομένα σας, τη δουλειά σας και τους αγαπημένους σας από δυσάρεστα γεγονότα.
Σας προτείνουμε να ακολουθήσετε πιστά αυτόν τον οδηγό. Αν σας φαίνεται μεγάλος ή πολύπλοκος, ζητήστε από κάποιον με περισσότερη εμπειρία να σας βοηθήσει.

ΚΑΝΟΝΑΣ ΠΡΩΤΟΣ: Backup, BACKUP, BACKUP!

Δεν χρειάζεται να πούμε πολλά εδώ, είναι ο βασικότερος κανόνας τον οποίο θα πρέπει να ακολουθείτε ανεξαρτήτως αν κινδυνεύετε να επιμολυνθείτε από Ransomware ή όχι. Στην περίπτωση που έχετε πρόσφατο backup και επιμολυνθείτε από Ransomware, το μόνο που έχετε να κάνετε είναι να απομακρύνετε την επιμόλυνση και να επαναφέρετε τα δεδομένα σας από το backup.

Δυστυχώς η απλή προσθήκη ενός σκληρού δίσκου στον Η/Υ σας και τήρηση των backup εκεί κάθε τόσο, δεν είναι αρκετή. Ο λόγος είναι ότι τα Ransomware θα στοχεύσουν σε όλους τους τοπικούς δίσκους του Η/Υ και σε όλους τους δικτυακούς δίσκους (πολλές φορές και σε αυτούς που δεν έχουν γίνει map). Αυτό σημαίνει ότι τα backup σε τοπικά και απομακρυσμένα μέσα θα κρυπτογραφηθούν επίσης.

Οι λύσεις σε αυτήν την περίπτωση είναι δύο: α) Τήρηση του backup σε Cloud με ό,τι αυτό συνεπάγεται (κόστος, πρόβλημα με την εχεμύθεια, αργή πρόσβαση) και β) Τήρηση του backup σε έναν δίσκο ο οποίος δεν είναι στο δίκτυο και αποσυνδέεται μετά την ολοκλήρωση του backup από τον Η/Υ.

ΚΑΝΟΝΑΣ ΔΕΥΤΕΡΟΣ: Εγκαταστήστε ένα καλό λογισμικό προστασίας

Σιγουρευτείτε ότι ο Η/Υ σας προστατεύεται από αξιόπιστο λογισμικό προστασίας. Προτείνουμε να εγκατασταθούν λογισμικά antivirus, antiransomware και antiexploit τα οποία να έχουν τη δυνατότητα ανάλυσης της συμπεριφοράς του υπολογιστή και να σας ενημερώνουν αν εντοπίσουν μόλυνση από Ransomware, ακόμα και αν αυτοί είναι νέοι (zero day tolerance).

ΚΑΝΟΝΑΣ ΤΡΙΤΟΣ: Εγκαταστείτε πάντα τις ενημερώσεις του λειτουργικού συστήματος

Οι πιο πολλοί Ransomware εγκαθίστανται μέσω scripts τα οποία ονομάζονται exploit kits. Αυτά στοχεύουν σε αδυναμίες και τρύπες ασφαλείας του λειτουργικού συστήματος του Η/Υ (πχ. των Windows). Αν λαμβάνετε ειδοποίηση από τα Windows ότι υπάρχουν ενημερώσεις, **εγκαταστήστε τις.** Πολλές από αυτές τις ενημερώσεις αφορούν την ασφάλεια και σας προστατεύουν από κενά ασφαλείας, τα οποία θα προστατεύσουν τον Η/Υ από το να εκτελεί εντολές του επιτιθέμενου.

Η Microsoft δημοσιεύει ενημερώσεις στο Patch Tuesday, το οποίο είναι κάθε δεύτερη Τρίτη κάθε μήνα, οπότε να είστε έτοιμοι να κάνετε αυτές τις ενημερώσεις και να επανεκκινήσετε τον Η/Υ σας εκείνη τη μέρα.

Τα υπόλοιπα λειτουργικά συστήματα, όπως τις Apple ή οι διανομές Linux δημοσιεύουν ενημερώσεις όποτε αυτές είναι απαραίτητες, οπότε να είστε προετοιμασμένοι να τις εγκαταστήσετε μόλις δημοσιευτούν.

ΚΑΝΟΝΑΣ ΤΕΤΑΡΤΟΣ: Διατηρείτε τα εγκατεστημένα προγράμματα ενημερωμένα

Ακριβώς όπως με τα λειτουργικά συστήματα, τα exploit kits στοχεύουν σε κενά ασφαλείας σε κοινώς χρησιμοποιούμενα λογισμικά και προγράμματα του Η/Υ, όπως η Java, ο Adobe Flash Player, ο Adobe Reader και άλλα. Επομένως είναι απολύτως αναγκαίο να τηρείτε τα εγκατεστημένα προγράμματα ενημερωμένα.

Για Windows, προτείνουμε το Flexera Personal Software Inspector, το οποίο θα κάνει έλεγχο των εγκατεστημένων προγραμμάτων και λογισμικών και θα σας ενημερώνει όταν υπάρχουν ανανεώσεις.

Για Mac, προτείνουμε το MacUpdate Desktop, το οποίο όμως δεν είναι δωρεάν.

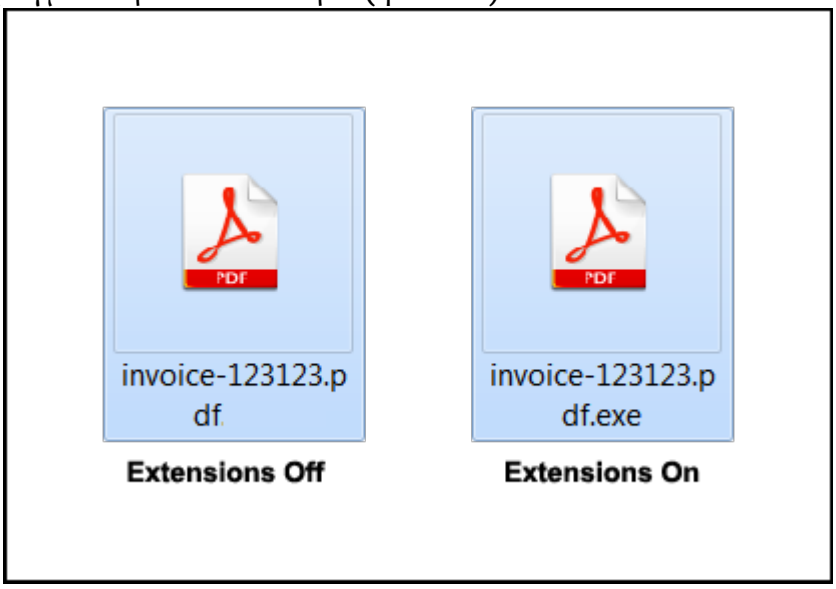
ΚΑΝΟΝΑΣ ΠΕΜΠΤΟΣ: Βεβαιωθείτε ότι τα φίλτρα SPAM σας είναι λειτουργικά

Ίσως η πιο διαδεδομένη μέθοδος διασποράς Ransomware είναι μέσω SPAM emails τα οποία παριστάνουν πως είναι δελτία αποστολής, τιμολόγια, βιογραφικά σημειώματα κλπ. Αν χρησιμοποιείτε web mail παρόχους όπως η Gmail, η Yahoo και η Hotmail, τότε τα περισσότερα από αυτά τα email φιλτράρονται πριν φτάσουν στο Inbox σας. Δυστυχώς αν έχετε δικό σας domain και η υπηρεσία του SPAM filtering δεν λειτουργεί σωστά, πολλά από αυτά τα email θα καταλήξουν στα εισερχόμενά σας.

ΚΑΝΟΝΑΣ ΕΚΤΟΣ: Ενεργοποιήστε την προβολή των επεκτάσεων των αρχείων!

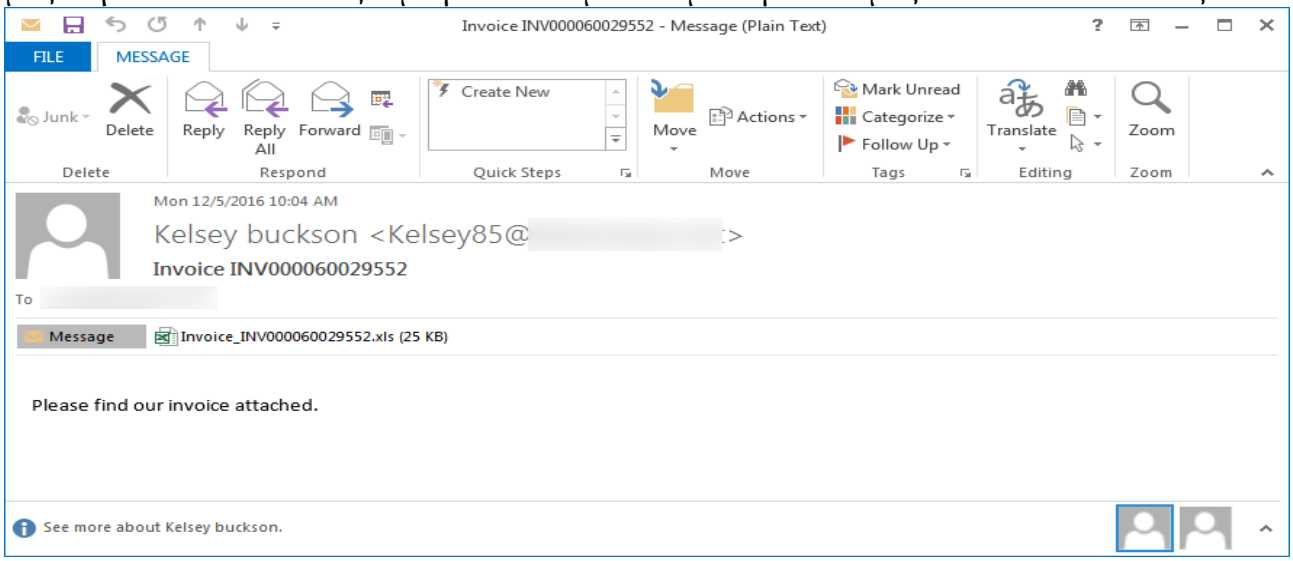
Ως προεπιλογή, τα Windows και τα MacOS δεν δείχνουν την επέκταση των αρχείων όταν περιηγήστε σε έναν φάκελο. Αυτό βοηθάει τους επιτιθέμενους στο να ξεγελάσουν τον χρήστη κάνοντας τον να νομίζει ότι ένα εκτελέσιμο αρχείο είναι στην πραγματικότητα ένα πιο οικείο αρχείο όπως ένα αρχείο Word, Excel ή PDF. Το θύμα θα ανοίξει το αρχείο

περιμένοντας να δει περιεχόμενο, όμως στην πραγματικότητα αυτό που κάνει είναι να εκτελεί το αρχείο που θα εγκαταστήσει το Ransomware.
Στην παρακάτω εικόνα φαίνεται ένα παράδειγμα όπου ένα κακόβουλο εκτελέσιμο αρχείο (.exe) παριστάνει ότι είναι .pdf. Με την ενεργοποίηση της προβολής των επεκτάσεων βλέπουμε την πραγματική του ταυτότητα (.pdf.exe).

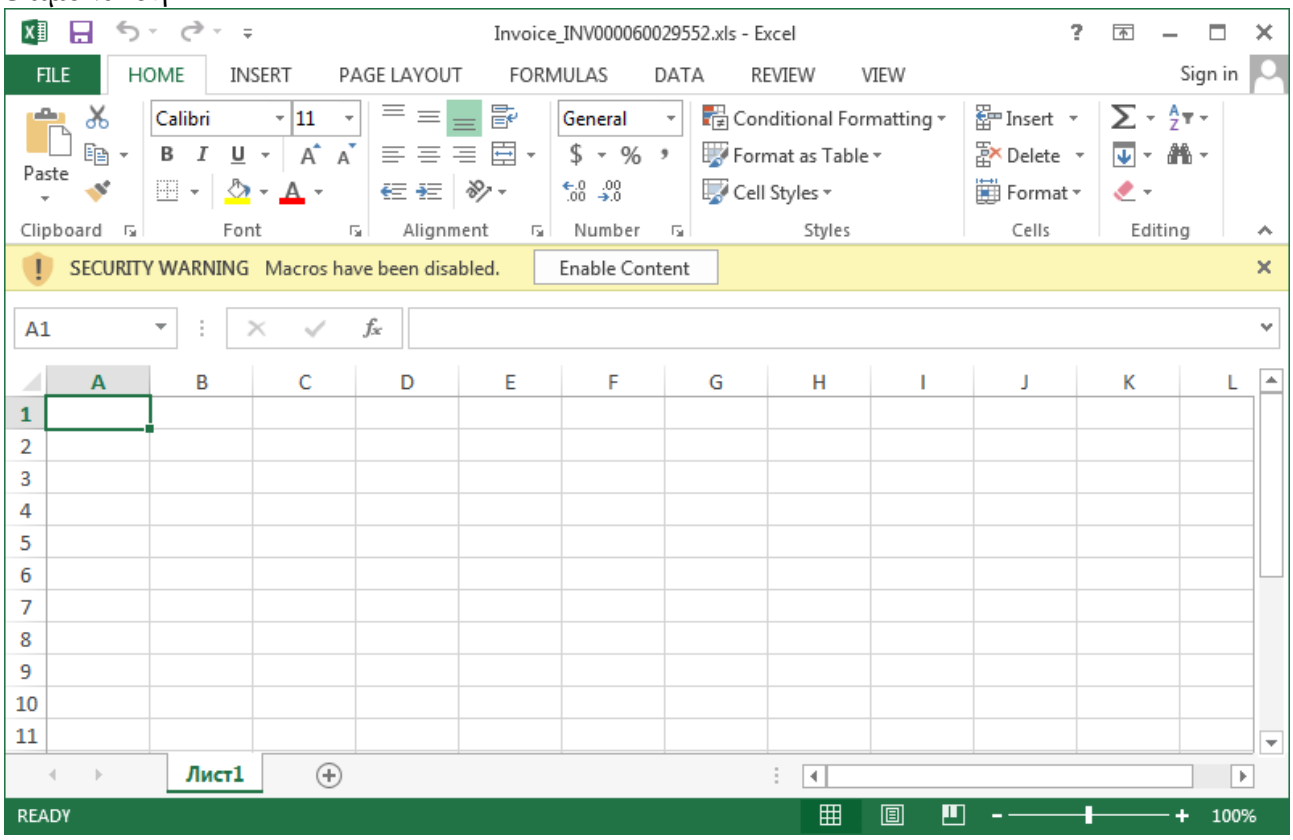


ΚΑΝΟΝΑΣ ΕΒΔΟΜΟΣ: Μην ανοίγετε επισυναπτόμενα αν δεν γνωρίζετε την προέλευσή τους

Με την επιμόλυνση από Ransomware μέσω SPAM email, είτε η ίδια η επιμόλυνση είτε ο downloader μέσω του οποίου κατεβαίνει η επιμόλυνση στον Η/Υ σας, βρίσκεται στα επισυναπτόμενα.
Αν λάβετε ένα email που περιέχει επισυναπτόμενο και δεν γνωρίζετε είτε γιατί το έστειλαν σε εσας, είτε τον αποστολέα, **μην το ανοίξετε.**
Στην παρακάτω εικόνα φαίνεται ένα email με επισυναπτόμενο το οποίο περιέχει τον Locky Ransomware. Όπως βλέπουμε, έχει ένα .xls επισυναπτόμενο (άρα φαινομενικά αθώο) και μας παρακινεί να το ανοίξουμε για να δούμε το τιμολόγιο που μας αποστέλλει κάποιος.



Αν κάνετε το λάθος και ανοίξετε το επισυναπτόμενο και δείτε μία προτροπή να ενεργοποιήσετε τις μακροεντολές ή το περιεχόμενο (Enable Macros ή enable Content), **μην το κάνετε**, γιατί αυτό θα κατεβάσει τον Ransomware στον Η/Υ σας και θα ξεκινήσει την επιμόλυνση.



ΚΑΝΟΝΑΣ ΟΓΔΟΟΣ: Προσέχετε τι κατεβάζετε και από που.

Τα δωρεάν downloads από το Internet, από Torrents και από P2P συνδέσεις μπορεί να ακούγονται δελεαστικά, όμως συχνά κρύβουν δυσάρεστες Ransomware εκπλήξεις. Να προσέχετε πάντα να κατεβάζετε από ιστοσελίδες που εμπιστεύεστε και να προσέχετε που πατάτε ΟΚ.

ΚΑΝΟΝΑΣ ΕΝΑΤΟΣ: Μετονομάστε το vssadmin στα Windows

Τα Shadow Copies χρησιμοποιούνται από τα Windows για να αποθηκεύουν αυτόματα Backup ή προηγούμενες εκδόσεις των αρχείων. Αυτά τα backup βοηθάνε στο να ανακτώνται δεδομένα που έχουν μεταβληθεί ή αλλοιωθεί.
Δυστυχώς οι δημιουργοί των Ransomware είναι αρκετά καλοί γνώστες αυτής της λειτουργίας, με αποτέλεσμα μία από τις πρώτες ενέργειες που κάνουν μόλις ξεκινήσει η επιμόλυνση είναι η διαγραφή όλων εκδόσεων των shadow copies εκτελώντας την εντολή vssadmin.exe.
Αν δεν έχετε λογισμικά που βασίζονται στο vssadmin προτείνουμε να το μετονομάσετε.

Για να μετονομάσετε το vssadmin θα πρέπει να "τρέξετε" το παρακάτω script:

```
@echo off
REM We are redirecting the output of the commands and any errors to NUL.
REM If you would like to see the output, then remove the  2>NUL from the end of the commands.

REM Check if vssadmin.exe exists. If not, abort the script

if NOT exist %WinDir%\system32\vssadmin.exe (
 echo.
 echo.%WinDir%\system32\vssadmin.exe does not exist!
 echo.
 echo Script Aborting!
 echo.
 PAUSE
 goto:eof
)

REM Check if the script was started with Administrator privileges.
REM Method from http://stackoverflow.com/questions/4051883/batch-script-how-to-check-for-admin-rights

net session >nul 2>&1

if %errorLevel% NEQ 0 (
```

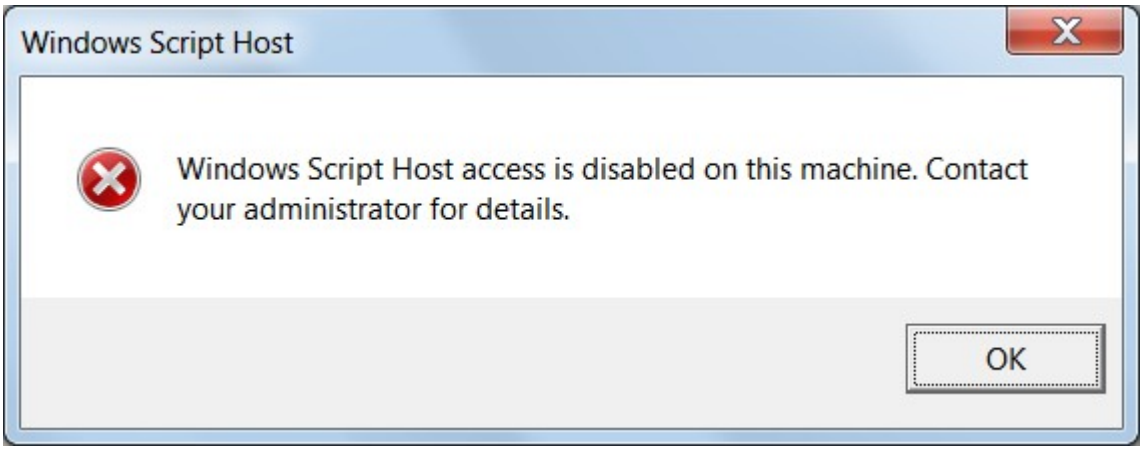
```
      set RenFile=vssadmin.exe-%%c-%%b-%%a-%%m%%n%%o%%p
   )
)

REM Rename vssadmin.exe to the filename in the RenFile variable

ren %WinDir%\system32\vssadmin.exe %RenFile% >nul 2>&1

REM Check if the task was completed successfully

if exist %WinDir%\system32\%RenFile% (
 echo.
 echo vssadmin.exe has been successfully renamed
 echo to %WinDir%\system32\%RenFile%.
 pause
) else (
 echo.
 echo There was a problem renaming vssadmin.exe
 echo to %WinDir%\system32\%RenFile%.
 echo.
 pause
)
:END
```

ΚΑΝΟΝΑΣ ΔΕΚΑΤΟΣ: Απενεργοποιήστε το Windows Script Host

Πολλές Ransomware επιμολύνσεις εγκαθίστανται μέσω επισυναπτόμενων τα οποία είναι script γραμμένα σε JS ή VBS.
Αν γνωρίζετε τι είναι αυτά, έχει καλώς.
Αν όχι, προτείνουμε να απενεργοποιήσετε τη δυνατότητα εκτέλεσης τέτοιων αρχείων στα Windows.

Για να το κάνετε αυτό, ακολουθήστε τις οδηγίες της Microsoft από εδώ:
https://technet.microsoft.com/en-us/library/ee198684.aspx

Αν το κάνετε αυτό και προσπαθήσει να εκτελεστεί script τέτοιου τύπου, θα λάβετε αυτήν την ειδοποίηση:



ΚΑΝΟΝΑΣ ΕΝΔΕΚΑΤΟΣ: Απενεργοποιήστε το Windows Powershell

Ομοίως με προηγουμένως, το PowerShell χρησιμοποιείται από τους επιτιθέμενους με σκοπό την εγκατάσταση των Ransomware ή ακόμα και την κρυπτογράφηση αρχείων.

Αν δεν το χρησιμοποιείτε, απενεργοποιήστε το. Για να το κάνετε αυτό, πηγαίνετε
Έναρξη> Γράψτε CMD> Enter
και δώστε την ακόλουθη εντολή στο Command Prompt:

```
powershell Set-ExecutionPolicy -ExecutionPolicy Restricted
```

Αν θέλετε να το ενεργοποιήσετε και πάλι, αλλάξτε από την παραπάνω εντολή το Restricted σε Unrestricted.

ΚΑΝΟΝΑΣ ΔΩΔΕΚΑΤΟΣ: Χρησιμοποιείτε πολύπλοκους κωδικούς ασφαλείας

Πάντα να χρησιμοποιείτε πολύπλοκους, δύσκολους κωδικούς. Ξεχάστε τα 12345, 0000, 15101969 κ.ο.κ. Αντ' αυτών, χρησιμοποιείτε κωδικούς όπως 1@4t6Y!&87kM-=^

ΚΑΝΟΝΑΣ ΔΕΚΑΤΟΣ ΤΡΙΤΟΣ: Απενεργοποιήστε το Remote Desktop των Windows ή αλλάξτε την προεπιλεγμένη θύρα του

Αν δεν χρησιμοποιείτε το Remote Desktop, **απενεργοποίηστε το.** Είναι ένας από τους πιο διαδεδομένους τρόπους εισβολής στον Η/Υ σας.

Αν το χρησιμοποιείτε και το χρειάζεστε, αλλάξτε την θύρα που χρησιμοποιεί για την επικοινωνία με τον έξω κόσμο.

Για να το κάνετε αυτό:
΄Εναρξη> Γράψτε REGEDIT>Enter

Στο παράθυρο που θα ανοίξει πηγαίνετε στο:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp και βρείτε την εγγραφή **PortNumber** στην δεξιά πλευρά του παραθύρου. Με διπλό κλικ επιλέξτε το, και στο παράθυρο που θα σας ανοίξει επιλέξτε Decimal και αλλάξτε το Value Data από 3389 σε ό,τι θέλετε εσείς.

ΣΥΝΟΨΗ

Ακολουθώντας αυτές μας τις οδηγίες θα έχετε θωρακίσει τον Η/Υ σας σε τεράστιο βαθμό.

Στην δυσάρεστη περίπτωση που έχετε μολυνθεί από Ransomware, **ΜΗ ΠΛΗΡΩΣΕΤΕ ΤΑ ΛΥΤΡΑ ΚΑΙ ΕΛΑΤΕ ΣΕ ΕΠΙΚΟΙΝΩΝΙΑ ΜΑΖΙ ΜΑΣ ΑΜΕΣΑ!**

Northwind Data Recovery
Αθήνα: Νίκης 30, 2ος όροφος, πλ. Συντάγματος, ΤΚ. 10557 τηλ. 2103314829
Θεσσαλονίκη: Γεωργ. Παπανδρέου 45, πρώην Ανθέων, ΤΚ. 54646 τηλ. 2310402675
Research Facilities: Λασκαράτου 7, ΤΚ 54646 τηλ. 2310402675 (εσωτ. 303-304-305)