ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

CERTCOOP

ΤΕΧΝΙΚΟ ΕΓΧΕΙΡΙΔΙΟ

ΑΣΦΑΛΟΥΣ ΡΥΘΜΙΣΗΣ ΚΑΙ ΧΡΗΣΗΣ WINDOWS 10 ΠΡΟΣΩΠΙΚΟΥ ΥΠΟΛΟΓΙΣΤΗ

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

./.

ΚΕΦΑΛΑΙΟ «Α»
ΕΙΣΑΓΩΓΗ

ΤΜΗΜΑ 1
ΓΕΝΙΚΑ

Στα θέματα ασφαλείας προσωπικών υπολογιστών υπάρχει ένας κανόνας, **δεν υπάρχει απόλυτη ασφάλεια**. Αυτό που υπάρχει είναι η λήψη μέτρων, η υιοθέτηση σωστής χρήσης του προσωπικού υπολογιστή, η συνεχής ενημέρωση και η συνεχής επαγρύπνηση, που μας επιτρέπουν να μετριάσουμε τον κίνδυνο.

Σκοπός αυτού του εγχειριδίου είναι αρχικά να δώσει γενική γνώση σε θέματα ασφαλείας αλλά και ειδική τεχνική γνώση, ανάλογα με το λειτουργικό σύστημα του καθενός, με τελικό στόχο την προστασία των προσωπικών υπολογιστών. Δεν πρόκειται για μία πολιτική ασφαλείας, αλλά για ενημερωτικό υλικό με στόχο την ενημέρωση των χρηστών σε προσωπικό επίπεδο για τους κινδύνους που διατρέχουν.

Απαντώντας στην ερώτηση "*μα δεν έχω κάτι αξίας στον υπολογιστή, γιατί να δεχτώ επίθεση;*" περιγράφουμε την **αξία ενός προσωπικού υπολογιστή για έναν κακόβουλο χρήστη.**

Ο υπολογιστής μας, σήμερα αποτελεί στόχο κακόβουλων χρηστών, για να χρησιμοποιηθεί σε κάθε είδους παράνομη δραστηριότητα. Είναι γεγονός πως η σύγχρονη ανάγκη για επικοινωνία επιβάλλει την χρήση δικτυακών συσκευών όπως υπολογιστές, tablet, κινητά και συνέπεια αυτού είναι να διακινούνται καθημερινά μια πληθώρα ψηφιακών πληροφοριών για εμάς, την οικογένειά μας, την εργασία μας και τις συνήθειές μας. Αυτές οι πληροφορίες , όπως και ο ίδιος υπολογιστής έχουν μεγάλη αξία, κυρίως οικονομική, για έναν εισβολέα.

Παρακάτω αναλύονται οι επιδιωκόμενοι στόχοι των κακόβουλων χρηστών, με την αντίστοιχη επεξήγηση.

1. Υποκλοπή ονομάτων χρηστών και κωδικών

Η υποκλοπή των ονομάτων χρήστη και των κωδικών του που χρησιμοποιεί στις διάφορες ιστοσελίδες στο διαδίκτυο, μπορούν να δώσουν πρόσβαση σε:

α. Τραπεζικούς λογαριασμούς, όπου μπορούν να δουν την οικονομική μας κατάσταση (έσοδα – έξοδα), να κάνουν μεταφορά χρημάτων σε άλλον λογαριασμό ή αγορά προϊόντων με πιστωτικές κάρτες, εν αγνοία μας.

β. Λογαριασμούς αγοραπωλησιών, όπως Amazon, Walmart, e-Bay, όπου μπορούν να κάνουν αγορές ή και πωλήσεις προϊόντων και αγαθών, εν αγνοία μας.

γ. Υπηρεσίες φύλαξης αρχείων, όπως iCloud, Google Drive, Dropbox, όπου μπορούν να αποκτήσουν πρόσβαση σε ότι είδους αρχεία φυλάσσουμε εκεί.

δ. Χρηματοοικονομικές υπηρεσίες, όπως ενεχυροδανειστήρια ή μετοχές, με τις αντίστοιχες δυνατότητες.

ε. Φορολογικά δεδομένα, όπου μπορούν να δουν την φορολογική μας ενημερότητα, περιουσιακά στοιχεία (αυτοκίνητα, κύρια κατοικία, εξοχικά, σκάφη), εισοδήματα παρελθόντων ετών, αριθμό μελών οικογενείας κλπ.

στ. Λογαριασμούς εταιρειών courier, όπως UPS, Fedex, όπου μπορούν να αποστείλουν κλεμμένα ή παράνομα αγαθά στο όνομά μας ή να παραλάβουν παραγγελίες που έγιναν για εμάς σε άλλη διεύθυνση.

2. Συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου (e-mail)

Εάν αποκτήσει κάποιος πρόσβαση στο ηλεκτρονικό μας ταχυδρομείο, τότε μπορεί:

α. Να ελέγξει τις επαφές μας, όπου συνήθως υπάρχουν και άλλα καταχωρημένα στοιχεία, όπως τηλέφωνα, διευθύνσεις και ιδιότητες για κάθε μία επαφή.

β. Να δει την προσωπική μας αλληλογραφία, χωρίς την έγκρισή μας.

γ. Να κάνει πολλαπλές προηγμένες απάτες με χώρες του εξωτερικού.

δ. Να συλλέξει πληροφορίες για αγορές, συνήθειες και προτιμήσεις μας, όπως πχ ταξίδια, μαγειρική, ηλεκτρονικές συσκευές κλπ, όπου μπορεί να μας προωθήσει αντίστοιχα προϊόντα για να τα αγοράσουμε.

ε. Να μάθει πληροφορίες που αφορούν στην υγεία μας, με στόχο την εκμετάλλευση αυτών προς όφελός του.

στ. Να μάθει πληροφορίες για τις ερωτικές μας προτιμήσεις, είτε σε αγορές είτε σε συντρόφους και μετά να μας εκβιάζει.

ζ. Να αποκτήσει πληροφορίες για την εταιρεία που εργαζόμαστε, από ανταλλαγές αλληλογραφίας, ώστε να μάθει πληροφορίες εκ των έσω, εν αγνοία μας.

Τα παραπάνω μπορεί να μην είναι άμεσα χρήσιμα σε αυτόν που θα πάρει τις συγκεκριμένες πληροφορίες, αλλά κάποιοι άλλοι τρίτοι, πληρώνουν

αδρά για να αποκτήσουν πρόσβαση σε τέτοια δεδομένα, όπως πχ διαφημιστικές εταιρείες, κατάσκοποι κλπ.

3. Υποκλοπή εικονικών προϊόντων και αγαθών (virtual goods)

Η πρόσβαση τρίτων σε εικονικά προϊόντα και αγαθά μπορεί να οδηγήσει:

α. **Στην πώληση** των εικονικών χαρακτήρων, αγαθών ή νομισμάτων από on-line παιχνίδια εις βάρος δικό μας και όσων έχουν πρόσβαση εκεί.

β. **Στην πώληση** οποιασδήποτε άδειας λογισμικού ή λειτουργικού συστήματος έχουμε αποκτήσει νόμιμα.

4. **Χρήση του υπολογιστή μας ως διαδικτυακό ρομπότ για παράνομες δραστηριότητες** (botnet - Δίκτυο υπολογιστών ελεγχόμενο κεντρικά και που εκτελεί αυτοματοποιημένες εργασίες μέσω του Διαδικτύου).

Ο υπολογιστής μας μπορεί να γίνει θύμα δραστηριότητας αυτοματοποιημένων προγραμμάτων (trojan) που ελέγχονται από τους κακόβουλους χρήστες μέσω botnet, με σκοπό:

α. Την αποστολή ανεπιθύμητης αλληλογραφίας, εν αγνοία μας, αλλά με το όνομά μας, σε εκατομμύρια χρήστες σε όλο τον κόσμο.

β. Την χρήση του ως μέλος μιας ευρείας διαμοιρασμένης επίθεσης άρνησης υπηρεσιών (DDOS) σε ιστοσελίδες και υπηρεσίες, εν αγνοία μας, αλλά με την υπογραφή μας.

γ. Την χρήση του υπολογιστή μας ως μέρος μια καλοστημένης απάτης που κατευθύνει ανυποψίαστους χρήστες, σε ανύπαρκτες υπηρεσίες που συνδέονται με εμάς, χωρίς την άδεια μας και τελικό σκοπό παράνομες δραστηριότητες.

δ. Την χρήση του υπολογιστή μας, ως ενδιάμεσο ή τελικό κόμβο ενός δικτύου διακομιστών μεσολάβησης (proxy server) για ανώνυμη (από την πλευρά του κακού) πλοήγηση στο Διαδίκτυο, αφού στην πραγματικότητα καταγράφεται η δική μας ηλεκτρονική διεύθυνση.

ε. Την αυτόματη επίλυση των εικόνων απεικόνισης ασφαλείας CAPTCHA για παράνομη πρόσβαση σε δικτυακούς τόπους (ιστοσελίδες), εν αγνοία μας.

5. Μίμηση της διαδικτυακής ταυτότητας μας

Ο κακόβουλος χρήστης μπορεί να αποκτήσει πρόσβαση στην διαδικτυακή μας ταυτότητα και να κάνει διαδικτυακές απάτες ή να την πουλήσει κάνοντας χρήση των:

α. Λογαριασμών μας σε κάποιο (ή όλα) από τα Facebook, Twitter, LinkedIn, Google+ κλπ, όπου έχουμε αναπτύξει τις διαδικτυακές μας γνωριμίες και φιλίες.

β. Των λογαριασμών ηλεκτρονικού μας ταχυδρομείου (e-mail).

γ. Των λογαριασμών προγραμμάτων επικοινωνίας, όπως Skype, Messanger, Viber κλπ.

6. Προσωπικός Εκβιασμός

Εάν ο υπολογιστής μας έχει πέσει θύμα κακόβουλου χρήστη, τότε αυτός μπορεί να απαιτήσει να μας εκβιάσει είτε για κάποιο χρηματικό ποσό, είτε για άλλες υπηρεσίες, είτε για εκδίκηση με:

α. Φωτογραφίες που τυχόν βρει στον υπολογιστή μας και μας εκθέτουν.

β. Φωτογραφίες που μπορεί να πάρει με τη χρήση της κάμερας του υπολογιστή μας, εν αγνοία μας.

γ. Κρυπτογράφηση μέρους αρχείων ή ολόκληρου του σκληρού μας δίσκου, ώστε να μην είναι προσπελάσιμα αυτά από εμάς.

δ. Καταγραφή των ιστοσελίδων που επισκεπτόμαστε και την απειλή δημοσιοποίησης τους.

ε. Αλλαγή των κωδικών πρόσβασης στους διαδικτυακούς λογαριασμούς μας.

στ. Την προβολή ψεύτικων αποτελεσμάτων ελέγχου αντιικών προγραμμάτων (Fake antivirus).

7. Χρήση του προσωπικού μας υπολογιστή ως Διακομιστής δικτύου

Ο υπολογιστής μας μπορεί να μετατραπεί σε διακομιστή δικτύου, εν αγνοία μας, και να χρησιμοποιηθεί:

α. Ως ξενιστής ιστοσελίδων υποκλοπής προσωπικών δεδομένων τρίτων.

β. Ως ξενιστής λογισμικού επιθέσεων ή κακόβουλου λογισμικού.

γ. Ως διακομιστής πειρατικού (παράνομου) υλικού, όπως αρχείων μουσικής, ταινιών, λογισμικού ή παιδικής πορνογραφίας.

Όπως μπορούμε να διαπιστώσουμε, υπάρχουν πάρα πολλοί λόγοι, για τους οποίους κάποιος άγνωστος προς εμάς, ενδιαφέρεται για τον προσωπικό μας υπολογιστή. Στην συνέχεια περιγράφουμε τον τρόπο με τον οποίο μπορεί κάποιος να αποκτήσει πρόσβαση σε έναν υπολογιστή.

ΤΜΗΜΑ 2
ΤΕΧΝΙΚΕΣ ΑΠΟΚΤΗΣΗΣ ΠΡΟΣΒΑΣΗΣ

Για να αποκτήσει κάποιος κακόβουλος χρήστης πρόσβαση σε έναν υπολογιστή θα πρέπει να εφαρμόσει μία από τις παρακάτω τεχνικές:

Εκμετάλλευση αδυναμιών (Server Side Exploitation). Κάθε εφαρμογή, λειτουργικό σύστημα και γενικά κάθε πρόγραμμα δεν είναι τίποτα άλλο από χιλιάδες γραμμές κώδικα. Οι κακόβουλοι χρήστες αναζητούν αδυναμίες στις γραμμές κώδικα, τις οποίες εκμεταλλεύονται για να αποκτήσουν πρόσβαση σε ένα πληροφοριακό σύστημα, ξεπερνώντας έτσι τα συστήματα και μέτρα ασφαλείας.

Brute Forcing (Επαναλαμβανόμενη δοκιμή συνθηματικών). Αν κάποιος έχει αδύναμο συνθηματικό ή συνθηματικό μια λέξη που βρίσκεται σε ένα λεξικό, τότε εύκολα κάποιος κακόβουλος χρήστης μπορεί να “μαντέψει” το συνθηματικό με την χρήση αυτόματων εργαλείων (ncrack, Hydra, medusa).

Επίθεση τελικού χρήστη (Client side attack). Με αυτή την τεχνική ένας επιτιθέμενος μπορεί να ξεπεράσει τα συστήματα ασφαλείας που έχει ένα δίκτυο ή ένας απλός χρήστης και με την εκμετάλλευση μιας αδυναμίας είτε στον Browser, είτε στον email client, είτε στις εφαρμογές που καλεί ο Browser και ο email client.

Social engineering είναι μία τεχνική που χρησιμοποιείται για να παραπλανηθεί ένας χρήστης, να κάνει μία ενέργεια που κάτω από άλλες συνθήκες δεν θα έκανε και έτσι ο επιτιθέμενος να αποκτήσει πρόσβαση στον υπολογιστή του και κατά συνέπεια στο δίκτυο.

Αντίμετρο σε αυτές τις επιθέσεις είναι η καθημερινή ενημέρωση τόσο σε προσωπικό επίπεδο όσο και σε επίπεδο προγραμμάτων.

Ο καλύτερος τρόπος να προστατευτούμε από κυβερνοεπιθέσεις είναι να διαθέτουμε δύο υπολογιστές. Ένας “γυμνός” δεν θα έχει τίποτα αποθηκευμένο και θα έχει απλά έναν φυλλομετρητή για πλοήγηση στο διαδίκτυο, θα έχει antivirus και firewall και όλες τις ενημερώσεις. Ο δεύτερος υπολογιστής δεν θα συνδεθεί ποτέ στο διαδίκτυο, θα έχει όλες τις απαραίτητες εφαρμογές για να εργαστούμε, θα έχει antivirus και firewall, τα οποία μπορούν να ενημερωθούν εκτός δικτύου (offline updates). Επιθυμητό θα ήταν να αποσυνδέσουμε και κάθε υλικό (κάρτες δικτύου - bluetooth) που πραγματοποιούν συνδέσεις.

Βασικό είναι να διαθέτουμε μία προσωπική πολιτική ασφαλείας και σωστής χρήσης του υπολογιστή μας, τόσο στον χώρο εργασία μας όσο και στο σπίτι μας, που θα περιλαμβάνει τους παρακάτω κανόνες:

1. Χρησιμοποιούμε μόνο νόμιμο λογισμικό ή λογισμικό ανοικτού κώδικα (Open Source), για να μπορούμε να πραγματοποιούμε τις ενημερώσεις (updates).

2. Ενημερώνουμε καθημερινά το λογισμικό με τις τελευταίες ενημερώσεις ασφαλείας (Security Updates, Patches, κλπ) ή αντικαθιστούμε το λογισμικό κάθε φορά με την νεώτερη έκδοσή του.

3. Χρησιμοποιούμε λογισμικό προστασίας (Anti-Virus, Firewall και Anti-Spyware), τα οποία ενημερώνουμε καθημερινά.

4. Χρησιμοποιούμε πολύπλοκα Συνθηματικά (Passwords), διαφορετικά σε κάθε λογαριασμό ή εφαρμογή και δεν είναι λέξη που περιλαμβάνετε σε λεξικό.

5. Δεν αποθηκεύουμε Συνθηματικά σε αρχεία του Η/Υ ή στον φυλλομετρητή (Browser) και δεν τα αποκαλύπτουμε σε κανέναν.

6. Δεν ακολουθούμε (κάνουμε κλικ) τους συνδέσμους-διευθύνσεις (Links-URLs) που μας αποστέλλονται με EMail ή Instant Messaging, αν δεν είμαστε σίγουροι για τον αποστολέα και την ασφάλεια του περιεχομένου.

7. Προσέχουμε τις διευθύνσεις (url) που πλοηγούμαστε, να είναι οι σωστές και όχι κάποιες παραπλανητικές.

8. Δεν ανοίγουμε επισυναπτόμενα αρχεία σε Emails, αν δεν είμαστε σίγουροι για την ασφάλεια του περιεχομένου.

9. Κρυπτογραφούμε προσωπικά και “ευαίσθητα” δεδομένα.

10. Ελέγχουμε συχνά τις εξωτερικές αποθηκευτικές συσκευές (π.χ. USB Drives) για μολυσμένα “αρχεία”.

11. Δεν αποθηκεύουμε, επεξεργαζόμαστε ή διακινούμε Διαβαθμισμένες πληροφορίες σε Αδιαβάθμητο δίκτυο (π.χ. Internet).

12. Προσέχουμε τα κοινωνικά δίκτυα, δεν αποκαλύπτουμε πληροφορίες που αφορούν την εργασία μας.

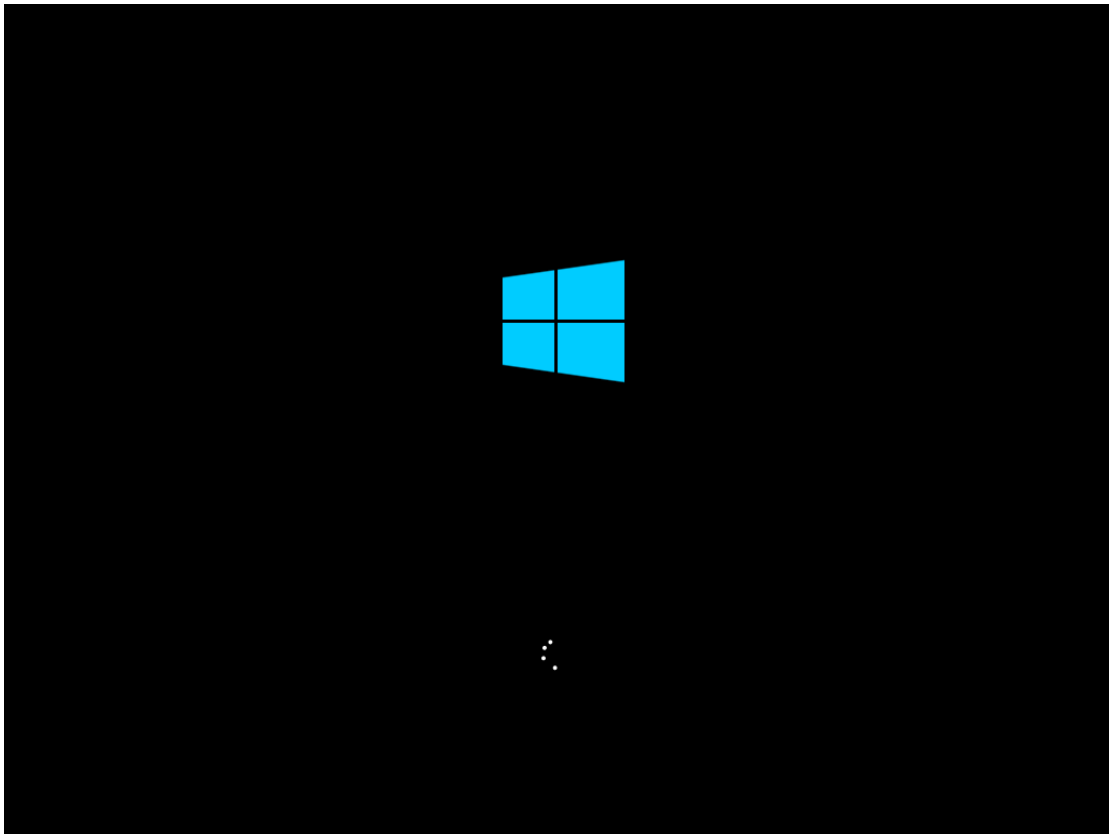
13. Αν για κάτι αμφιβάλλουμε, το απορρίπτουμε. Παράδειγμα, αν δεν είμαστε σίγουροι για το άνοιγμα ενός email, τότε το διαγράφουμε.

14. Αν μία εφαρμογή δεν την χρειαζόμαστε τότε την καταργούμε (απεγκατάσταση προγράμματος). Με αυτό τον τρόπο μειώνουμε την επιφάνεια επίθεσης στον υπολογιστή μας.

Τα κεφάλαια που ακολουθούν, περιγράφουν τα τεχνικά βήματα που πρέπει να ακολουθήσει κάποιος χρήστης για να αυξήσει την ασφάλεια του windows υπολογιστή του και να μετριάσει τον κίνδυνο από κυβερνοεπιθέσεις. Απόλυτη

ασφάλεια δεν υπάρχει, ωστόσο θα πρέπει να είμαστε σε θέση να αναγνωρίζουμε τις επιθέσεις και να τις αντιμετωπίζουμε έγκαιρα.

ΚΕΦΑΛΑΙΟ «Β»
ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΑΣΦΑΛΗ ΡΥΘΜΙΣΗ ΚΑΙ ΧΡΗΣΗ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ WINDOWS 10



ΤΜΗΜΑ 3
ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

Για την ασφάλεια των εφαρμογών μας αλλά και του λειτουργικού μας συστήματος, πρέπει να ακολουθούμε τις δύο βασικές αρχές:

Η αρχή των ελαχίστων προνομίων: κάθε οντότητα (η οποία θα μπορούσε να είναι ένας χρήστης, αλλά και ένα πρόγραμμα ή μια συσκευή) πρέπει να έχει πρόσβαση μόνο τις πληροφορίες ή τους πόρους που είναι απολύτως αναγκαίοι για την εκπλήρωση της εργασίας της.

Μείωση της επιθετικής επιφάνειας: Η επιφάνεια επίθεσης περιλαμβάνει το πεδίο της λειτουργικότητας που είναι διαθέσιμο σε έναν μη εξουσιοδοτημένο χρήστη, σε ένα δίκτυο ή σε έναν υπολογιστή. Όσο περισσότερο δικαιώματα έχει ο χρήστης τόσο αυξάνεται η επιθετική επιφάνεια. Όσο περισσότερες εφαρμογές έχουμε εγκατεστημένες, τόσο αυξάνεται η επιθετική επιφάνεια.

Πολύ σημαντικό να έχουμε **εγκατεστημένες** στον υπολογιστή μας μόνο **νόμιμες εφαρμογές**, όπως νόμιμο λειτουργικό σύστημα αλλά και το office. Μόνο έχοντας νόμιμες εφαρμογές, μπορούν αυτές να λαμβάνουν όλες τις κρίσιμες ενημερώσεις και να έχουμε σε υψηλό επίπεδο ασφαλείας τον υπολογιστή μας.

Η αρχή των ελαχίστων προνομίων

Για να εφαρμόσουμε την αρχή των ελαχίστων προνομίων δημιουργούμε έναν χρήστη με περιορισμένα δικαιώματα. Συνεπώς αν κάποιος κακόβουλος πάρει πρόσβαση στον υπολογιστή μας θα έχει τα ίδια περιορισμένα δικαιώματα. Αν θέλουμε κάτι, παράδειγμα, προσωπικά στοιχεία να τα προστατέψουμε ως απλός χρήστης, τότε τα προστατεύουμε με έναν άλλο λογαριασμό, που δεν χρησιμοποιούμε όταν συνδεόμαστε στο διαδίκτυο. Για να δυσκολέψουμε ακόμα περισσότερο τον επιτιθέμενο απενεργοποιούμε και το “run as”. Με λίγα λόγια έχουμε έναν λογαριασμό για να εργαζόμαστε όταν δεν είμαστε συνδεδεμένοι στο διαδίκτυο (offline) και έναν άλλον όταν είμαστε συνδεδεμένοι (online).

Μείωση της επιθετικής επιφάνειας

Η επιφάνεια επίθεσης περιλαμβάνει το σύνολο των δικαιωμάτων-δυνατοτήτων που είναι διαθέσιμο σε έναν μη εξουσιοδοτημένο χρήστη, σε ένα δίκτυο ή σε έναν υπολογιστή. Όσο περισσότερα δικαιώματα έχει ο χρήστης τόσο αυξάνεται η επιθετική επιφάνεια. Όσο περισσότερες εφαρμογές έχουμε εγκατεστημένες, τόσο αυξάνεται η επιθετική επιφάνεια. Με απλά λόγια, ρυθμίζουμε το σύστημά μας ώστε να είμαστε σε θέση να πραγματοποιούμε τις καθημερινές εργασίες μας, αυτό που χρειαζόμαστε δηλαδή και τίποτα άλλο. Αυτό συνεπάγεται πως αν μια δυνατότητα (εφαρμογή, υπηρεσία) των Windows δεν χρησιμοποιείται, δεν την χρειαζόμαστε, θα πρέπει να την απεγκαταστήσουμε ή να την απενεργοποιήσουμε. Συνεπώς έχουμε εγκατεστημένες ή ενεργοποιημένες μόνο τις υπηρεσίες ή τα προγράμματα που χρειαζόμαστε για να επιτελέσουμε την εργασία

μας.

Ο στόχος μας είναι να προστατεύσουμε τους υπολογιστές μας από κακόβουλες ενέργειες που ίσως συμβούν. Θα ασφαλίσουμε το σύστημα μας, προκειμένου να μειώσουμε την επιθετική μας επιφάνεια (attack surface) και να εμποδίσουμε τους κακόβουλους χρήστες, από το να παραβιάσουν το σύστημά μας.

Ρυθμίσεις εγκατάστασης λειτουργικού (Installation Settings windows 10)

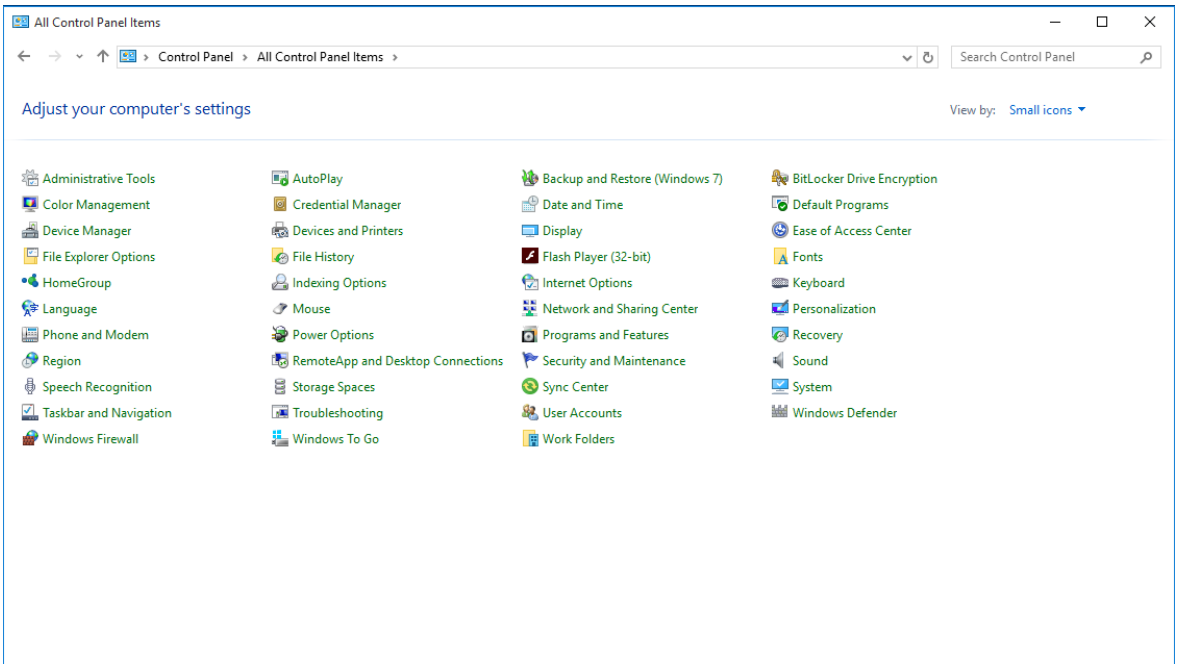
Για να εγκαταστήσουμε με ασφάλεια ένα λειτουργικό θα πρέπει να το κάνουμε **χωρίς να είμαστε συνδεδεμένοι** στο διαδίκτυο. Κατά την διάρκεια της εγκατάστασης ενός Windows 10 υπάρχει η σχετική επιλογή να μην “κατεβάζει” τις ενημερώσεις. Εάν έχουμε άλλο λειτουργικό και θέλουμε να κάνουμε upgrade σε windows 10, πρώτα κάνουμε upgrade για να κάνει αυτόματα ενεργοποίηση (activation). Στην συνέχεια εγκαθιστούμε εκ νέου το λειτουργικό, θα θυμάται την ενεργοποίηση (activation). Κατά την διάρκεια της εγκατάστασης επιλέγουμε τα ακόλουθα:

Μετά από μερικές επανεκκινήσεις (reboots), θα μας ζητήσει να κάνουμε τις προσωπικές μας ρυθμίσεις, κάνουμε click στο "Customized settings" στο κάτω μέρος της οθόνης και επιλέγουμε:

- **Personalize your speech, typing --> [off]**
- **Sending typing and inking data --> [off]**
- **Let apps use your advertising ID --> [on]**
- **Let Windows and apps request your location --> [off]**
- **Use smartscreen --> [on]**
- **Use page prediction --> [off]**
- **Automatically connect to open hotspots --> [off]**
- **Automatically conect to networks shared by your contacts --> [off]**

ΤΜΗΜΑ 4
ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΛΕΙΤΟΥΡΓΙΑΣ ΣΥΣΤΗΜΑΤΟΣ

Πριν ξεκινήσουμε τις ρυθμίσεις, καλό είναι να εμφανίσουμε όλες τις ρυθμίσεις στον πίνακα ελέγχου (Control Panel). Θα πρέπει να ρυθμίσουμε τον πίνακα ελέγχου να χρησιμοποιεί μικρά εικονίδια. Για να το επιτύχουμε αυτό, πάμε: **στο search (αναζητούμε control panel) --> Control Panel, επιλέγουμε 'View by: Small Icons'.** Με αυτή την επιλογή θα βλέπουμε όλες τις ρυθμίσεις.

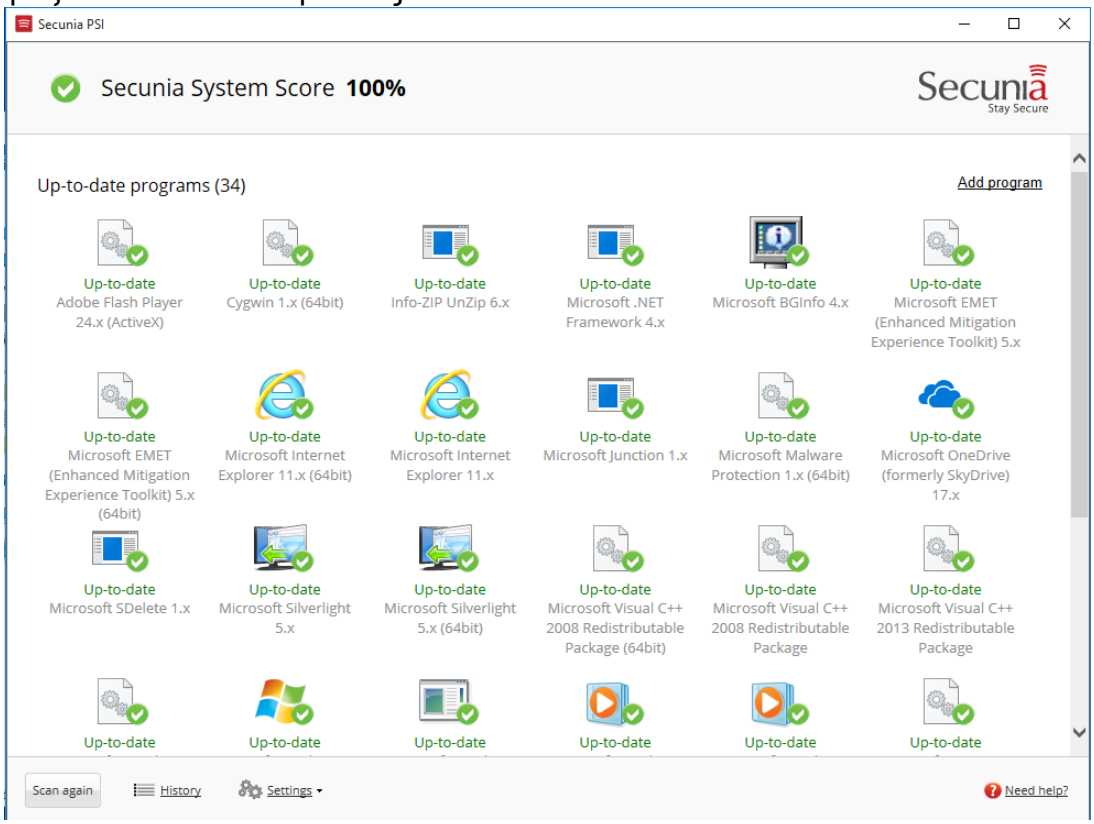


Ενημερώσεις συστήματος και εφαρμογών

Για να έχουμε ένα καλό επίπεδο ασφάλειας, θα πρέπει τόσο το λειτουργικό σύστημα, όσο και οι εφαρμογές, που είναι εγκατεστημένες στον υπολογιστή, να πραγματοποιούν καθημερινά ενημερώσεις. Θα πρέπει κάθε εφαρμογή να είναι νόμιμη, ώστε να μπορεί απρόσκοπτα να ενημερώνεται. Κάθε εφαρμογή, όπως

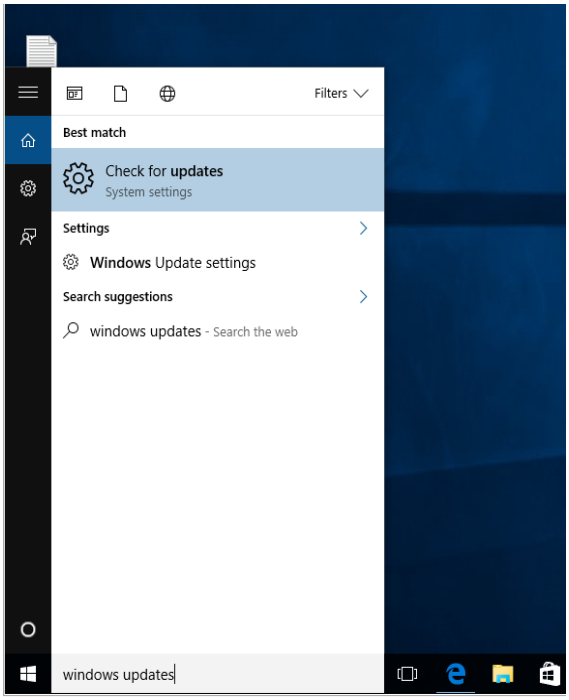
είναι και το λειτουργικό σύστημα, δεν είναι παρά γραμμές κώδικα. Ένας κακόβουλος χρήστης μπορεί να εντοπίσει αδυναμίες στον κώδικα, να “γράψει” ένα exploit και να ξεπεράσει με αυτό, όλα τα συστήματα ασφαλείας μας. Για να εξαλειφθούν αυτές οι αδυναμίες, οι διάφοροι κατασκευαστές λογισμικού, εκδίδουν ενημερώσεις περιοδικά ή κάθε φορά που εντοπιστεί μία αδυναμία.

Η **Secunia** μας δίνει δωρεάν μία εφαρμογή, την Personal Software Inspector (PSI),(http://secunia.com/vulnerability_scanning/personal/). Κάνοντας χρήση αυτού του λογισμικού, θα μας ενημερώνει κάθε φορά που κάποια από τις εφαρμογές μας χρειάζεται ενημέρωση ή υπάρχει μία νέα έκδοση. Προτείνετε η εγκατάστασή του. Έχοντας όλες τις εφαρμογές νόμιμες, το secunia μεταφορτώνει (downloading) και εγκαθιστά για εμάς, όλες τις ενημερώσεις των εφαρμογών καθώς και τις νέες εκδόσεις τους. Συνεπώς κρατά ενήμερο τον υπολογιστή μας και ανεβάζει το επίπεδο ασφαλείας του.

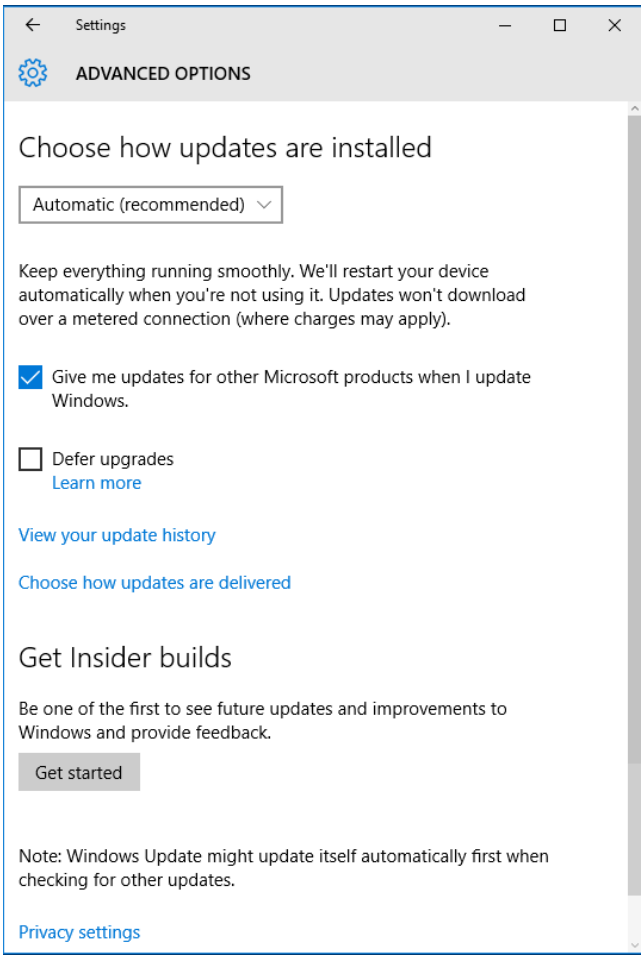


Εικόνα 1 . Secunia PSI (score 100%)

Στα Windows 10 για να έχουμε σε καθημερινό επίπεδο, ενήμερο το λειτουργικό σύστημα, ενεργούμε ως εξής: στη γραμμή αναζήτησης (**Search)** πληκτρολογούμε **Windows Update** και επιλέγουμε **windows update settings ή check for updates.**



Είναι σημαντικό **κάθε εφαρμογή** να είναι **ενήμερη**, όπως πχ το MS Office. Συνεπώς επιλέγουμε στις advanced ρυθμίσεις των windows updates να πραγματοποιεί ενημερώσεις και για άλλες εφαρμογές των windows.



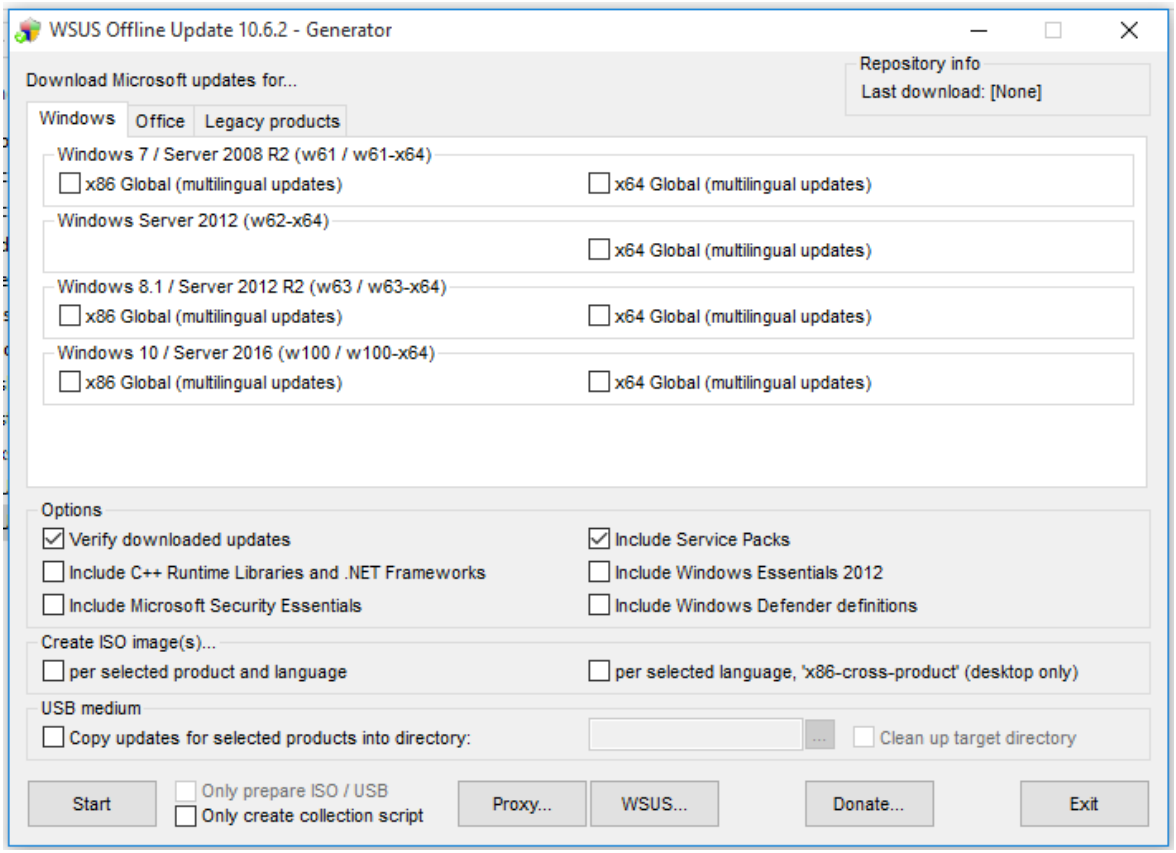
./.

Από την έκδοση των Windows 10, έχουν εκδοθεί σημαντικές - κρίσιμες ενημερώσεις. Στην περίπτωση που δεν έχουν εγκατασταθεί, θα μπορούσε την απουσία τους να την εκμεταλλευθεί κάποιος κακόβουλος χρήστης για να παραβιάσει τον υπολογιστή μας. Μία από τις τακτικές που εφαρμόζουν οι κακόβουλοι χρήστες είναι να εμποδίζουν και την αυτόματη ενημέρωση του λειτουργικού μας. Εμποδίζουν δηλαδή τον έλεγχο για ενημερώσεις (**Windows Check for Updates**). Συνεπώς στην περίπτωση που δεχόμαστε επίθεση στον υπολογιστή μας από κάποιον κακόβουλο χρήστη :

1. Είναι πολύ πιθανό να “εμποδίσει” το λειτουργικό σύστημα από το να λάβει και να εγκαταστήσει τις κρίσιμες ενημερώσεις (ρυθμίζει το λειτουργικό να μην κάνει αυτόματα ενημέρωση).

2. Είναι πολύ πιθανό επίσης να δεχτούμε επίθεση καθώς προσπαθούμε να λάβουμε και να εγκαταστήσουμε τις ενημερώσεις σε απευθείας σύνδεση (online).

Για να αποφύγουμε επίθεση κατά την διάρκεια εγκατάστασης του λειτουργικού, υπάρχει ένα δωρεάν εργαλείο που λέγεται WSUS Offline Update (http://www.wsusoffline.net/). Το λογισμικό αυτό “κατεβάζει” ενημερώσεις για όλες τις εκδόσεις των Windows και δημιουργεί ένα ISO image file. Απλά “καίμε” αυτό το ISO image file σε ένα DVD, το τοποθετούμε στον υπολογιστή μας και αυτό ξεκινά την εγκατάσταση των ενημερώσεων. Παρέχει μόνο τις κρίσιμες ενημερώσεις για το λειτουργικό σύστημα. Γι’ αυτό όταν έχουμε ολοκληρώσει την εγκατάσταση των κρίσιμων ενημερώσεων, θα πρέπει να πραγματοποιήσουμε έλεγχο για ενημερώσεις (Windows Check for Updates), προκειμένου να λάβουμε και τις απλά μη-κρίσιμες ενημερώσεις (non-critical updates). Επομένως, τρέχουμε το εργαλείο σε έναν άλλο υπολογιστή ώστε να “τραβήξει” τις ενημερώσεις και στη συνέχεια χρησιμοποιούμε το updates disc στον υπολογιστή που κάνουμε εγκατάσταση. Αφού “κατεβάσουμε” το WSUS Offline Update εργαλείο και αποσυμπιέσουμε το αρχείο του, πατάμε δεξί κλίκ και επιλέγουμε “Run as administrator”. Στη συνέχεια επιλέγουμε την πλατφόρμα την οποία θέλουμε να ενημερώσουμε και επιλέγουμε “Create ISO images 'per selected product and language'” . Τέλος, επιλέγουμε το Start button.



Μόλις τελειώσει, ελέγχουμε τον υποφάκελο iso, προκειμένου να εντοπίσουμε το ISO image file. Πρόκειται για ένα DVD image file. Κάνουμε δεξί κλίκ και επιλέγουμε 'Burn disc image'.

Εγκατάσταση των Service Packs Offline

Επιπρόσθετα, μπορούμε να κατεβάσουμε το/τα service pack(s), σε έναν διαφορετικό υπολογιστή από αυτόν που πραγματοποιείται η εγκατάσταση. Εν συνεχεία μπορούμε να τα αντιγράψουμε στον υπολογιστή που γίνεται η εγκατάσταση και να τα εγκαταστήσουμε.

Προσοχή!

Δεν επιτρέπουμε να συνδεθεί ο υπολογιστής στο δίκτυο, χωρίς να έχουμε εγκαταστήσει όλες τις κρίσιμες ενημερώσεις για κάθε εφαρμογή και για το λειτουργικό.

Εγκατάσταση Κρίσιμων και Σημαντικών Ενημερώσεων

Χρησιμοποιούμε το “updates disc”, το οποίο δημιουργήθηκε από το WSUS Offline Update και πραγματοποιούμε εγκατάσταση των κρισίμων ενημερώσεων (patches).

Τέλος πολύ σημαντικό είναι να επισκεπτόμαστε καθημερινά ιστοσελίδες που

μας ενημερώνουν για τις νέες τρωτότητες, ώστε να είμαστε ενήμεροι για τυχόν τρωτότητες που μπορεί να έχει το λειτουργικό μας σύστημα, αλλά και οι εγκατεστημένες εφαρμογές μας. Αν διαπιστώσουμε για παράδειγμα πως ο Internet Explorer έχει μία διαπιστωμένη αδυναμία/τρωτότητα για την οποία δεν έχουν εκδοθεί ενημερώσεις ασφαλείας, τότε πρέπει να εργαζόμαστε με άλλον browser, μέχρι να αποκατασταθεί το πρόβλημα (να εγκαταστήσουμε τις ενημερώσεις ασφαλείας).

Σχετικοί σύνδεσμοι:
http://technet.microsoft.com/en-us/security/bulletin
http://www.securityfocus.com/
http://en.wikipedia.org/wiki/Exploit_%28computer_security%29
http://www.securiteam.com/
http://www.exploit-db.com/
http://www.wsusoffline.net/
http://www.exploitalert.com/

ΤΜΗΜΑ 5
ΑΡΧΙΚΗ ΠΑΡΑΜΕΤΡΟΠΟΊΗΣΗ ΛΕΙΤΟΥΡΓΙΚΟΎ ΣΥΣΤΉΜΑΤΟΣ

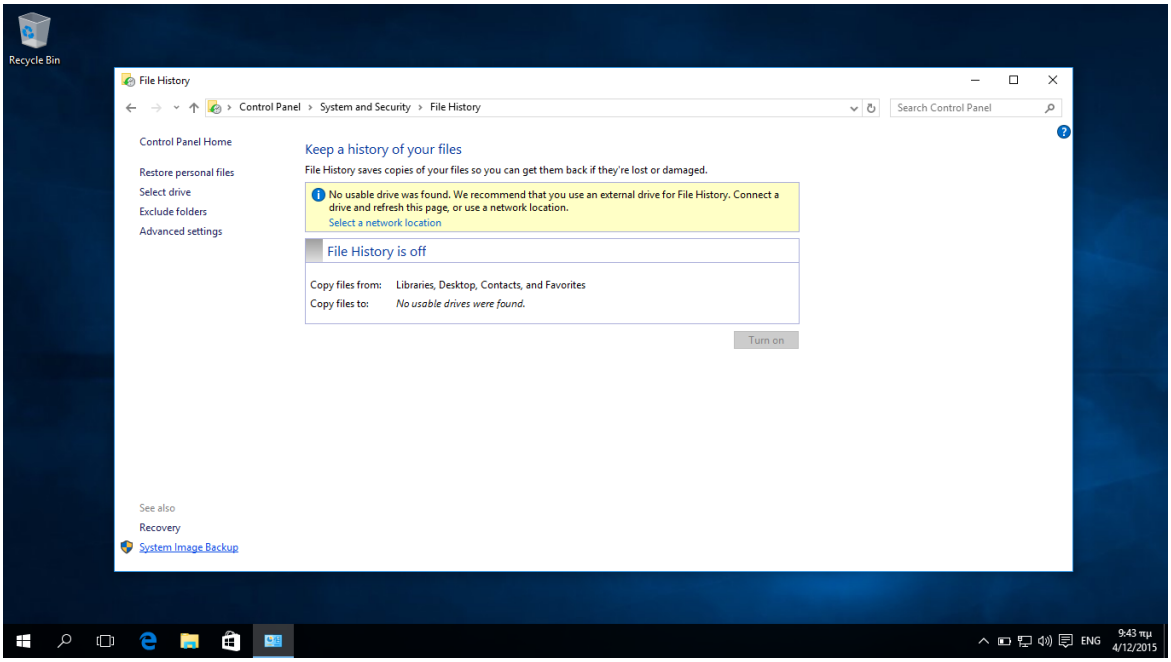
Δημιουργία αντιγράφου ασφαλείας

Το πρώτο βήμα μετά την εγκατάσταση του λειτουργικού συστήματος και μόλις ολοκληρώσουμε όλες τις ενημερώσεις, για όλα τα προγράμματα, είναι η δημιουργία αντιγράφου ασφαλείας. Η διαδικασία στα Windows 10 είναι διαφορετική από ότι στα Windows 7.

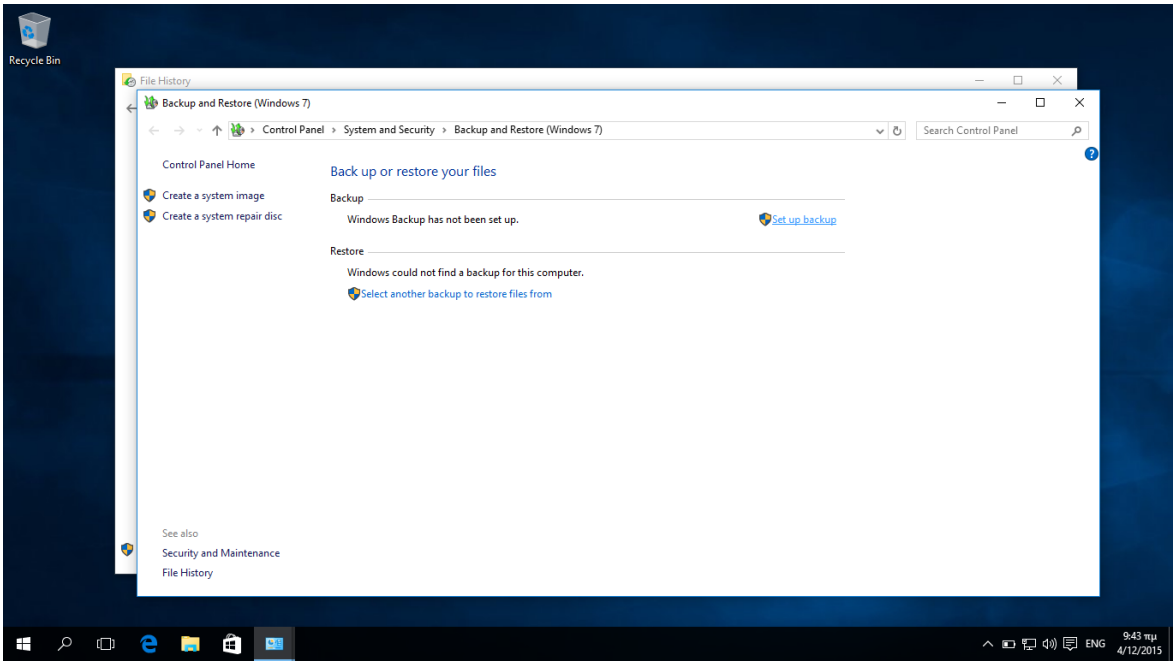
Για να δημιουργήσουμε ένα αντίγραφο ασφαλείας μπορούμε να χρησιμοποιήσουμε την ενσωματωμένη υπηρεσία του λειτουργικού συστήματος **File History** ακολουθώντας την παρακάτω διαδικασία:

Γράφουμε στο search box, **File History**, κάνουμε κλικ στο **file history** και μετά επιλέγουμε **System Image Backup**.

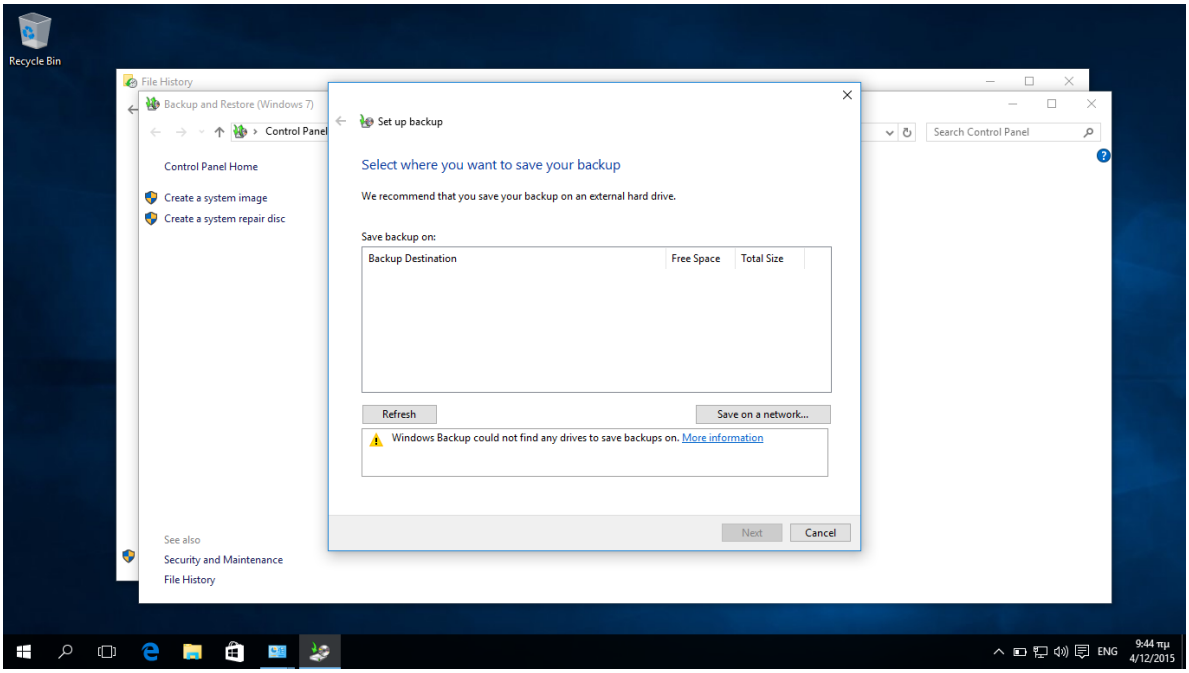
Στη συνέχεια επιλέγουμε (κάτω αριστερα) **System Image Backup**



Στο επόμενο παράθυρο επιλέγουμε **Create a system image**



Τελειώνοντας επιλέγουμε την τοποθεσία που θα δημιουργηθεί το αντίγραφο ασφαλείας.



Για να χρησιμοποιήσουμε το backup image του συστήματός μας και να επαναφέρουμε τον υπολογιστή μας, επιλέγουμε το μενού ρυθμίσεων (Settings menu) της νέας εγκατάστασης των Windows 10 και πηγαίνουμε στο Ενημέρωση & αποκατάσταση (Update & recovery). Κάτω απο το Recovery βρίσκουμε το Advanced startup και κάνουμε κλικ στο κουμπί Επανεκκίνηση τώρα (Restart now). Μετά την επανεκκίνηση του υπολογιστή μας, πηγαίνουμε στο αντιμετώπιση προβλημάτων (Troubleshoot), στην συνέχεια επιλογές για προχωρημένους (Advanced Options), και στη συνέχεια επιλέγουμε την ανάκτηση της εικόνας του συστήματος (System image recovery).

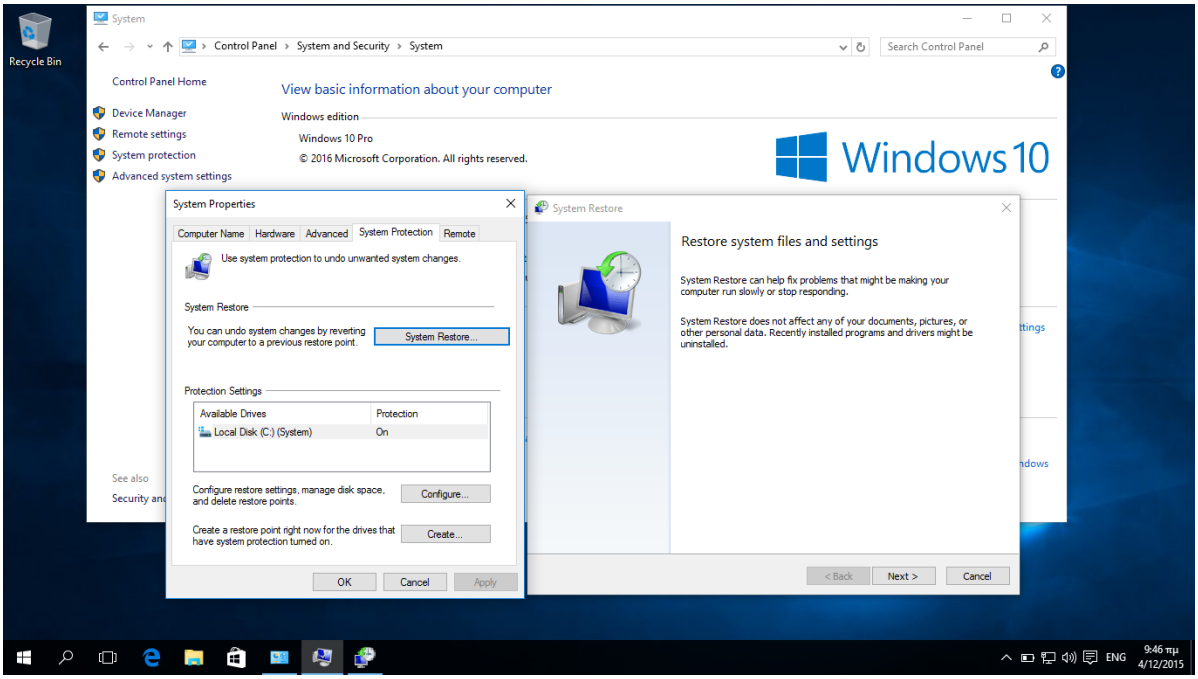
Υπάρχουν επίσης δωρεάν εφαρμογές που μπορούν να μας βοηθήσουν στο να πάρουμε αντίγραφο ασφαλείας όλου του σκληρού δίσκου και να κάνουμε ολοκληρωτική αποκατάσταση του λειτουργικού με μία καθαρή εικόνα (clean backup image). Τέτοιες εφαρμογές είναι το DriveImage XML (**http://www.runtime.org/driveimage-xml.htm**) και το paragon (http://www.paragonsoftware**.com/home/br-free/**). Πολύ καλό και απλό στην χρήση είναι το macrium reflect free edition (http://www.macrium.com/reflectfree.aspx)

Προσοχή

Δημιουργούμε το αντίγραφο ασφαλείας, ώστε στην περίπτωση που θεωρήσουμε πως έχουμε μολυνθεί από κάποιον ιό και δεν μπορούμε να τον αντιμετωπίσουμε αποτελεσματικά, τότε αποκαθιστούμε μία "καθαρή" εικόνα του υπολογιστή μας με την χρήση αυτού του αντιγράφου.

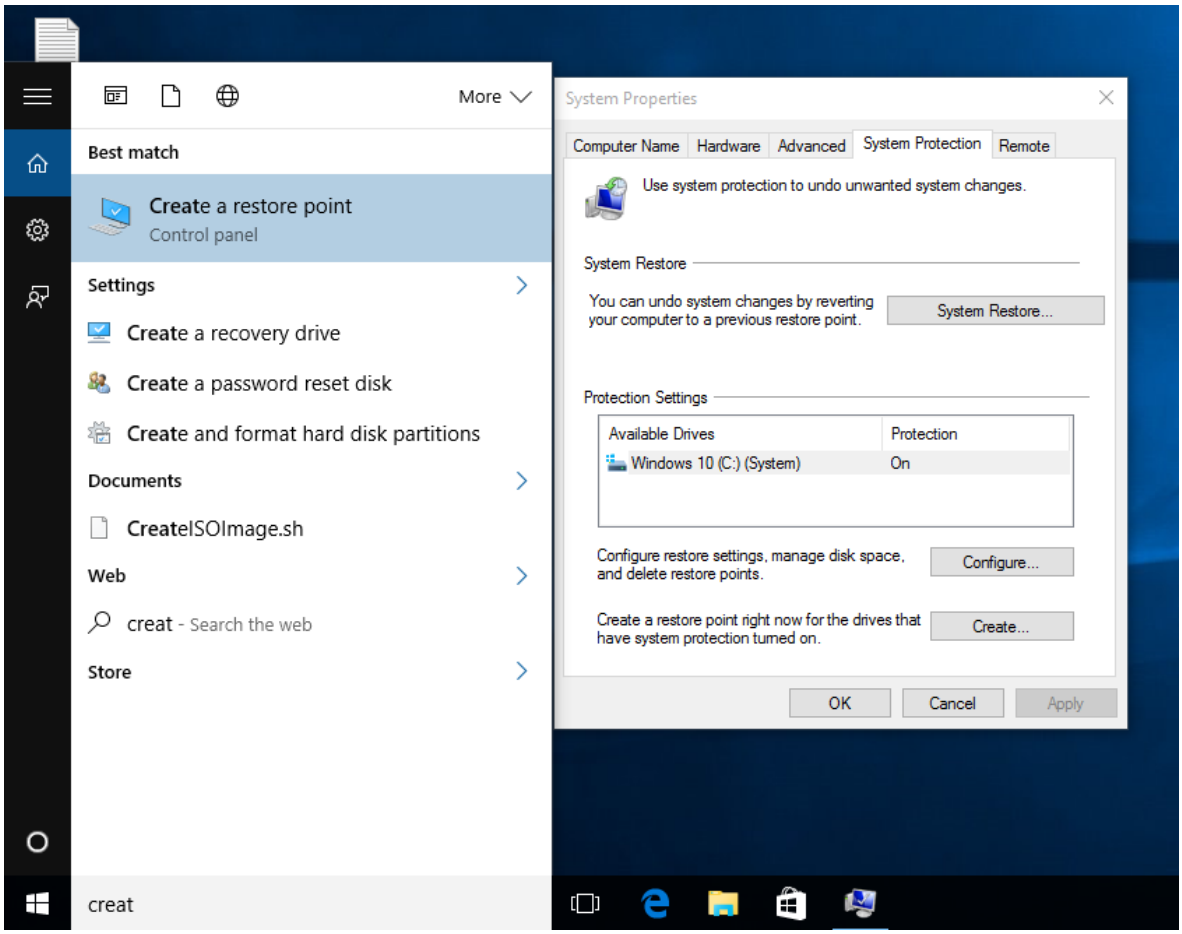
Ορισμός περιοδικών σημείων επαναφοράς

Για την αποφυγή της δημιουργίας συχνών ολικών αντιγράφων ασφαλείας, μπορούμε να κάνουμε χρήση των σημείων επαναφοράς για την προστασία των δεδομένων μας. Το λειτουργικό σύστημα δημιουργεί περιοδικά σημεία επαναφοράς χωρίς να χρειάζεται κάποια ενέργεια από τον χρήστη. Έτσι, επιλέγοντας την υπηρεσία **System Restore (Search --> Control Panel --> System and Security --> System Protection)** και πατώντας το **System Restore** έχουμε τη δυνατότητα να επιλέξουμε κάποιο από τα διαθέσιμα σημεία επαναφοράς που θεωρούμε ασφαλέστερο.



Μπορούμε να δημιουργήσουμε και εμείς σημεία αναφοράς χωρίς να περιμένουμε το λειτουργικό σύστημα να τα δημιουργήσει. Για να το κάνουμε αυτό γράφουμε στην αναζήτηση "Create a restore point" και το επιλέγουμε από την λίστα που μας εμφανίζεται.

Στην καρτέλα "System Protection" στο "System Properties", επιλέγουμε "Create".

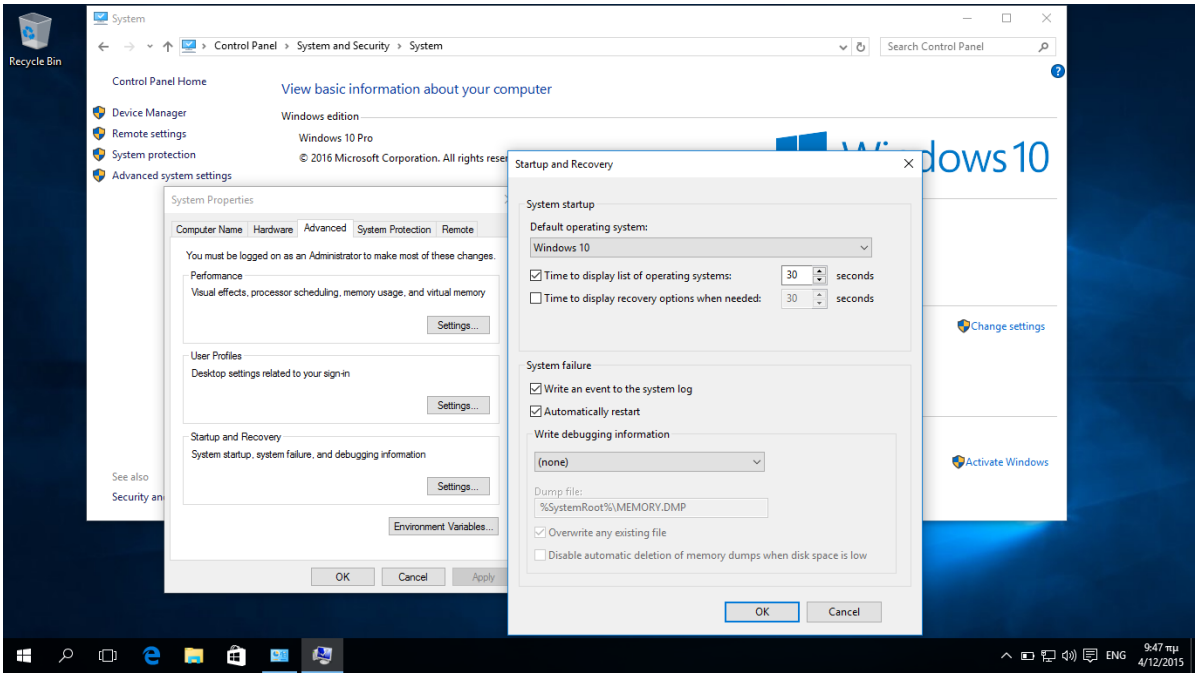


Απενεργοποίηση του dump file creation

Το λειτουργικό έχει την δυνατότητα να δημιουργεί αντίγραφα της φυσικής μνήμης αλλά και αντίγραφα της μνήμης μιας διεργασίας. Αυτά τα αντίγραφα μπορεί να τα εκμεταλλευτεί ένας κακόβουλος χρήστης για να μπορέσει να υποκλέψει χρήσιμες πληροφορίες όπως συνθηματικά που βρίσκονται στην μνήμη. Ενεργοποιούμε αυτή τη ρύθμιση μόνο όταν χρειάζεται και όταν υπάρχουν προβλήματα. Συνεπώς θα πρέπει να είναι απενεργοποιημένο για την καλύτερη προστασία του συστήματος. Για την απενεργοποίησης εργαζόμαστε ως εξής:

Απενεργοποίηση

Πάμε control panel > System and security > System > Advanced System Settings > Startup and Recovery Settings και στο **Write debugging information** επιλέγουμε **--> None.**

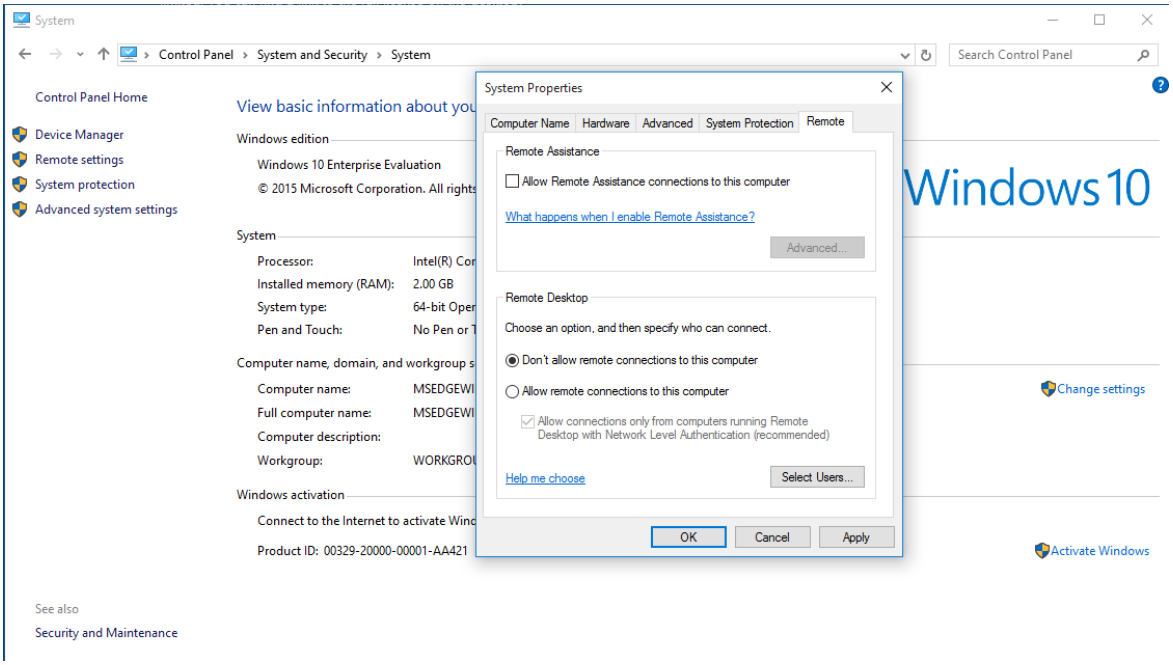


Απενεργοποίηση του Remote Assistance

Η απομακρυσμένη βοήθεια (Remote Assistance) δίνει την δυνατότητα σε κάποιον τρίτο να πάρει τον απομακρυσμένο έλεγχο του υπολογιστή μας (επιφάνεια εργασίας, πληκτρολόγιο, ποντίκι). Επιτρέπει μόνο σε 'προσκεκλημένους χρήστες' να πάρουν τον έλεγχο του υπολογιστή. Εφόσον δεν χρειαζόμαστε απομακρυσμένη βοήθεια θα πρέπει να την απενεργοποιήσουμε.

Απενεργοποίηση

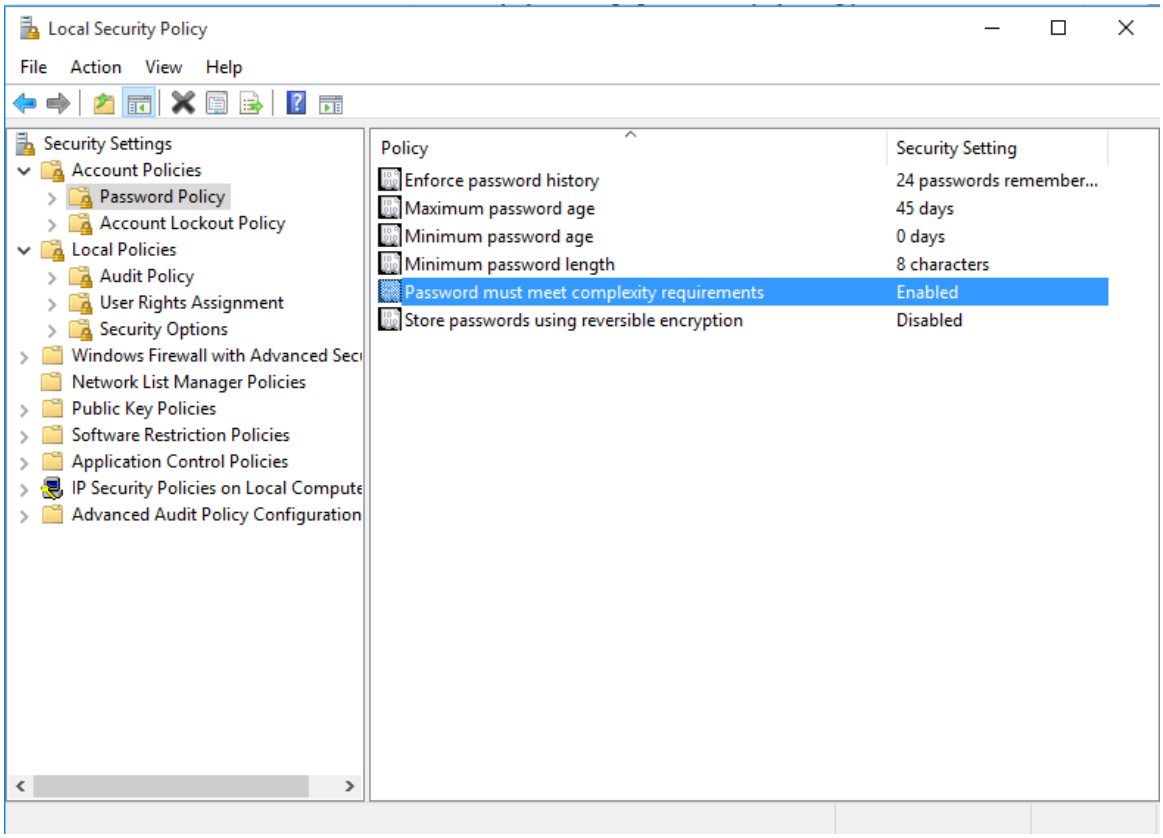
Πάμε control panel > System and security > System > Advanced System Settings >Remote tab και **αποεπιλέγουμε το** allow remote assistance



ΤΜΗΜΑ 6
ΡΥΘΜΙΣΕΙΣ ΧΡΗΣΤΩΝ

Ρύθμιση των συνθηματικών του χρήστη (password)

Θα πρέπει το συνθηματικό που επιλέγουμε να ικανοποιεί κάποιες βασικές απαιτήσεις ασφαλείας. Θα πρέπει να είναι πολύπλοκο, να έχει δηλαδή διάφορα σύμβολα (κεφαλαία–μικρά, ειδικούς χαρακτήρες και κενά), να έχει μήκος τουλάχιστον 8 χαρακτήρων, να μην είναι λέξη που υπάρχει σε λεξικό, ούτε κάποια ημερομηνία (πχ γέννησης), ενώ για κάθε λογαριασμό θα πρέπει να υπάρχει διαφορετικό συνθηματικό. Μια καλή πολιτική είναι να αλλάζουμε συνθηματικό συχνά (το πολύ κάθε 60 μέρες), να μην εφαρμόζουμε το ίδιο δεύτερη φορά και να κλειδώνει ο λογαριασμός μας μετά από 3 αποτυχημένες προσπάθειες σύνδεσης για 30 λεπτά. Ένα παράδειγμα ισχυρού συνθηματικού είναι: **Isx1r0_P@ssW0rd!@#.** Όλα τα παραπάνω μπορούμε να τα ρυθμίσουμε μέσα από τις ρυθμίσεις τοπικής πολιτικής. Για να ανοίξει η καρτέλα των τοπικών ρυθμίσεων ασφαλείας, γράφουμε στην αναζήτηση (search) “Local security policy” και επιλέγουμε “Account Policies” και στην συνέχει “Password Policy”. Ένα τυπικό στιγμιότυπο τοπικών ρυθμίσεων που αφορά το συνθηματικό χρήστη, φαίνεται στην επόμενη εικόνα:



Σχετικοί σύνδεσμοι:

windows.microsoft.com/en-us/**windows/change-windows-password**

http://en.wikipedia.org/wiki/Password_strength

Προσοχή

Δεν είναι καλή πρακτική να χρησιμοποιούμε τον ίδιο κωδικό παντού. Ιδιαίτερα και με την πεποίθηση ότι ένας ισχυρός κωδικός μας προστατεύει, είναι σύνηθες να χρησιμοποιείται ο ίδιος κωδικός σε πολλές υπηρεσίες, όπως e-mail, e-banking, facebook, windows log in, κ.α. Η ασφάλεια σε κάθε μία από τις υπηρεσίες αυτές όμως δεν είναι η ίδια. Αν ανακαλυφθεί ο κωδικός μας σε μία από αυτές, οδηγούμαστε στην απώλεια όλων των προσωπικών μας λογαριασμών και δεδομένων.

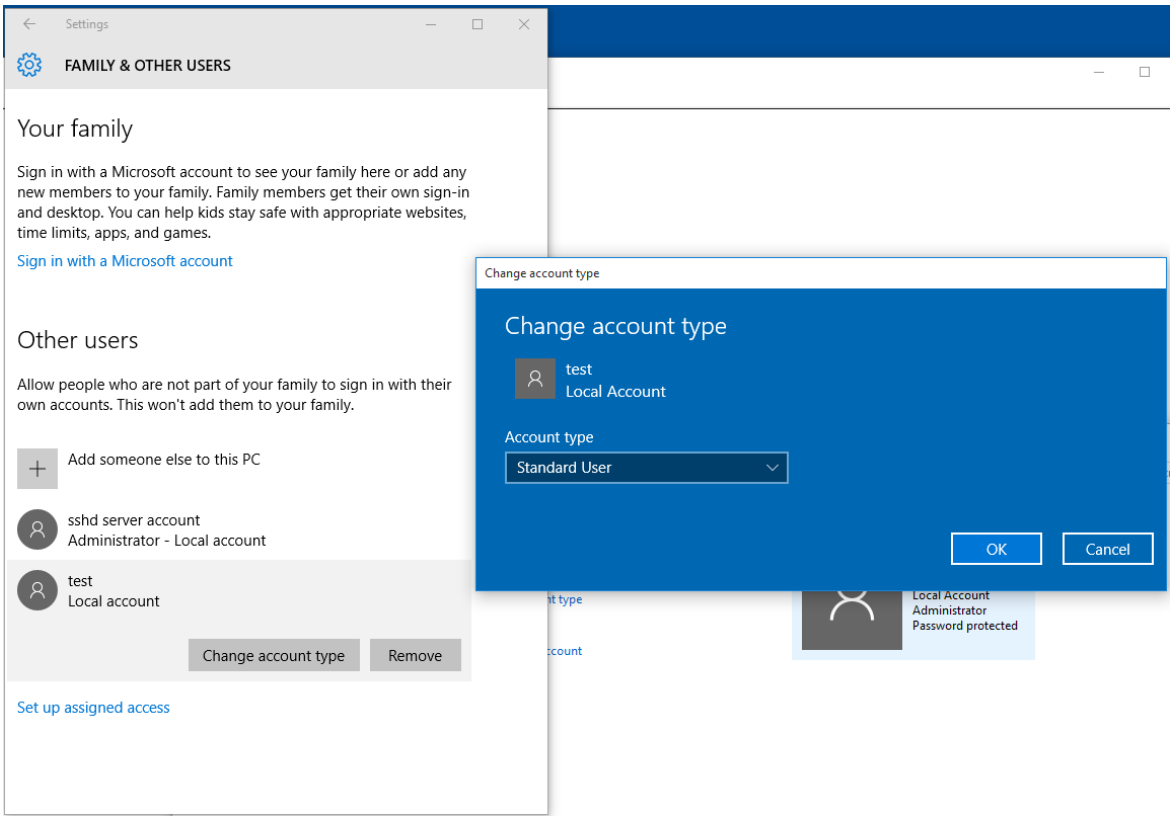
Δικαιώματα χρήστη

Όσο περισσότερα χαρακτηριστικά (υπηρεσίες, εφαρμογές) έχουμε ενεργοποιημένα / εγκατεστημένα τόσο μεγαλώνει η επιθετική επιφάνεια στον υπολογιστή μας (attack surface). Συνεπώς θα απαιτηθεί ιδιαίτερη προσπάθεια να προστατέψουμε το σύστημά μας. Μια ευπάθεια/αδυναμία αρκεί και για να δώσει τη δυνατότητα σε έναν επιτιθέμενο να αποκτήσει πρόσβαση στον υπολογιστή μας. Όσες περισσότερες εφαρμογές έχουμε εγκαταστήσει ή όσο περισσότερες υπηρεσίες είναι ενεργοποιημένες ενώ δεν χρειάζονται, τόσο περισσότερο αυξάνει η πιθανότητα εντοπισμού μιας αδυναμίας για απόκτηση πρόσβασης. Οι επιτιθέμενοι

γνωρίζουν τα πάντα σχετικά με τα κενά ασφαλείας και τα χρησιμοποιούν για να πραγματοποιήσουν κυβερνοεπιθέσεις. Γι' αυτό το λόγο απενεργοποιούμε τις υπηρεσίες που δεν απαιτούνται και εγκαθιστούμε μόνο τις εφαρμογές που χρειαζόμαστε.

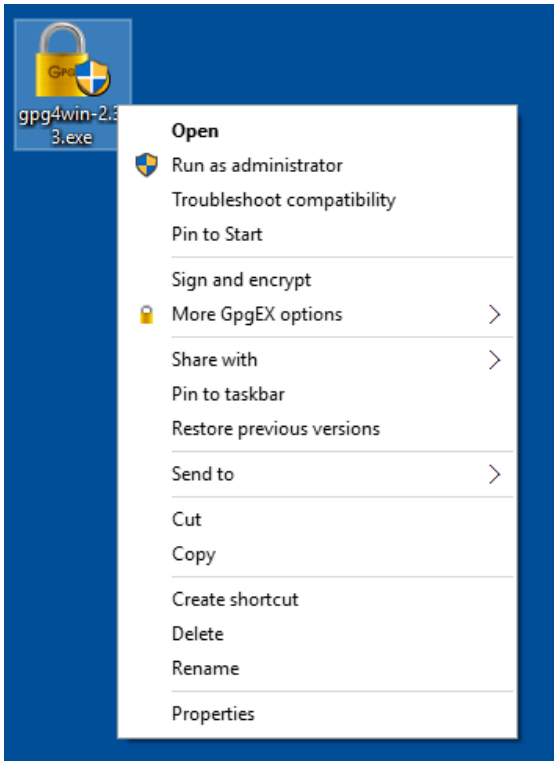
Όσο ισχυρό και να είναι το συνθηματικό μας, **δεν θα πρέπει ποτέ** να εργαζόμαστε στο διαδίκτυο με λογαριασμό χρήστη που έχει επαυξημένα δικαιώματα (έχει δικαιώματα διαχειριστή). Για το λόγο αυτό, δημιουργούμε έναν **χρήστη με περιορισμένα δικαιώματα** (standard user) και εργαζόμαστε πάντα με αυτό τον λογαριασμό. (Βλ. User Account Control). Στην περίπτωση που θέλουμε να εγκαταστήσουμε μία εφαρμογή και αυτή χρειάζεται administrator δικαιώματα, τότε κάνουμε δεξί κλικ πάνω στην εφαρμογή και επιλέγουμε **run as administrator**, όπως φαίνεται και στην παρακάτω εικόνα. Θα μας ζητηθεί να δώσουμε το συνθηματικό του administrator. Έτσι, με αυτό τον τρόπο, αποφεύγουμε την πιθανή εγκατάσταση ιομορφικού λογισμικού που απαιτεί πλήρη δικαιώματα ή εάν εγκατασταθεί θα έχει περιορισμένα δικαιώματα και το ιομορφικό λογισμικό.

Για να προσθέσουμε έναν χρήστη με περιορισμένα δικαιώματα, εργαζόμαστε ως εξής:
Επιλέγουμε Start > Settings > Accounts > Family & other people > Add someone else to this PC.



Στα windows 10 ο πρώτος λογαριασμός χρήστη έχει δικαιώματα διαχειριστή (δεν είναι διαχειριστής). Συνεπώς μια από τις πρώτες ενέργειές μας είναι η δημιουργία ενός απλού χρήστη (Standard user account) με περιορισμένα δικαιώματα. Χρησιμοποιούμε αυτόν τον λογαριασμό για την καθημερινή μας εργασία. Χρησιμοποιούμε τον λογαριασμό διαχειριστή (administrative account), μόνο για να πραγματοποιήσουμε εγκατάσταση προγραμμάτων, παραμετροποίηση δικτύου, ή συντήρηση συστήματος.

Όταν εργαζόμαστε μέσω ενός απλού λογαριασμού, κάθε ιομορφικό λογισμικό (malware) και κάθε επιτιθέμενος που θα αποκτήσει πρόσβαση στον υπολογιστή μας, θα προσπαθήσει να κληρονομήσει τα δικαιώματά μας. Δεν θα καταφέρει όμως τα αποκτήσει δικαιώματα διαχειριστή, ώστε να εφαρμόσει σημαντικές τροποποιήσεις στο σύστημά μας, αφού εμείς θα έχουμε δικαιώματα απλού χρήστη.Ένας απλός χρήστης για να κάνει αλλαγές στον υπολογιστή, θα χρειάζεται κάθε φορά το συνθηματικό του Administrator. Συνεπώς αν θέλει παράδειγμα να εγκαταστήσει μία εφαρμογή, θα κάνει δεξί κλικ πάνω της και θα επιλέξει **run as administrator** και αφού δώσει το συνθηματικό, μόνο και μόνο τότε θα εγκατασταθεί η εφαρμογή. Παράδειγμα στην εικόνα που ακολουθεί (Για να τρέξουμε το gpg4win με δικαιώματα διαχειριστή).



Προσοχή

Στο διαδίκτυο εργαζόμαστε μόνο με περιορισμένα δικαιώματα (standard user). Επίσης, δεν αφήνουμε ποτέ σημαντικά αρχεία στον υπολογιστή, μέσα από τον οποίο συνδεόμαστε στο διαδίκτυο, όπως λογαριασμούς,

συνθηματικά και οτιδήποτε δεν θέλουμε να μας υποκλαπή.

Ρύθμιση ενός Λογαριασμού της Microsoft (Microsoft Account)

Στα Windows 10, εάν σχεδιάζουμε να πραγματοποιήσουμε αγορές μέσω του “Windows app Store”, χρειάζεται να χρησιμοποιηθεί ένας λογαριασμός της Microsoft (**Microsoft Account)** για την σύνδεση (login) .

Επίσης για τον ίδιο σκοπό, μπορούμε να χρησιμοποιήσουμε ένα λογαριασμό Gmail ή yahoo mail ή outlook.com ή Hotmail.com. Εάν χρησιμοποιούμε κάποιον από τους παραπάνω, τα windows θα δημιουργήσουν ένα αντίγραφο του λογαριασμού (mirror account) στο outlook.com, ο οποίος θα χρησιμοποιεί το ίδιο όνομα και συνθηματικό χρήστη. Επιπλέον, θα ενσωματώνει τον τηλεφωνικό μας αριθμό σε αυτόν τον λογαριασμό. Ο τηλεφωνικός μας αριθμός χρησιμοποιείται σαν 2ο στάδιο αυθεντικοποίησης, όταν πρόκειται να πραγματοποιήσουμε αγορές.

Όμως **προσοχή**, δεν απαιτείται ο λογαριασμός του διαχειριστή (το συνθηματικό του) του υπολογιστή μας, να είναι ο ίδιος με τον λογαριασμό της Microsoft (“Windows app Store”), διότι το συνθηματικό βρίσκεται αποθηκευμένο και εκτίθεται μέσω του Outlook.com. Με αυτό τον τρόπο κάποιος μπορεί να το υποκλέψει από το διαδίκτυο (Outlook.com) και να δώσει την δυνατότητα στον κακόβουλο χρήστη να αποκτήσει πρόσβαση στον προσωπικό μας υπολογιστή, αφού “σπάσει” το κρυπτογραφημένο συνθηματικό.

Σε κάθε περίπτωση, πρέπει να κάνουμε οτιδήποτε, προκειμένου να κρατήσουμε ασφαλή τον MS account, αφού έχει αποθηκευμένο τον αριθμό της πιστωτικής μας κάρτας. Όταν χρησιμοποιούμε για πρώτη φορά το “Win Store” προκειμένου να πραγματοποιήσουμε μια αγορά, τα windows ζητούν τον αριθμό της πιστωτικής μας κάρτας και τον αποθηκεύουν απευθείας μέσα στον MS account. **Για μεγαλύτερη ασφάλεια**, είναι προτιμότερο να μην χρησιμοποιείται ο λογαριασμός αυτός για αποστολή ηλεκτρονικού ταχυδρομείου και να μην ενεργοποιείται το OneDrive. Ένας εκτεθειμένος MS account, θα δώσει την ευκαιρία σε ένα επιτιθέμενο να αποκτήσει πρόσβαση στα πάντα!

Ασφαλίζουμε πάντα τον λογαριασμό μας (MS account) με τη χρήση μιας ισχυρής πρότασης-συνθηματικού (passphrase). Όταν θέλουμε να ελέγξουμε τις συναλλαγές μας, μας ζητείται το passphrase. Επομένως, εάν το passphrase έχει παραβιαστεί, ο επιτιθέμενος μπορεί να συνδεθεί στον υπολογιστή μας και επιπλέον να πραγματοποιήσει αγορές. Ένας εναλλακτικός τρόπος αντιμετώπισης, είναι να αγοράσουμε τις εφαρμογές που επιθυμούμε και να πηγαίνουμε άμεσα στο outlook.com και να αφαιρούμε τα στοιχεία τις πιστωτικής κάρτας από το λογαριασμό.

Προσοχή

Δημιουργούμε λογαριασμό Microsoft, μόνο για τον διαχειριστή (Administrator) και ποτέ για τους χρήστες του υπολογιστή, προκειμένου να

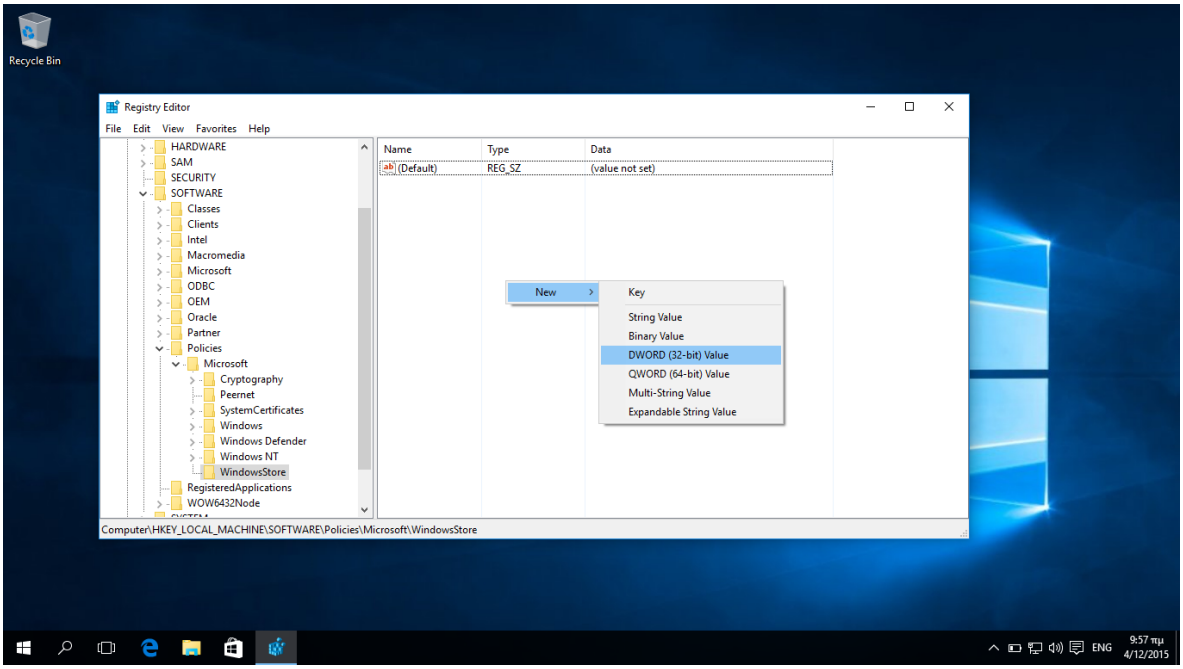
αποφύγουμε την έκθεση του υπολογιστή σε κινδύνους.

Εάν για οποιοδήποτε λόγο, χρησιμοποιήσουμε λογαριασμό Microsoft και για τους απλούς χρήστες, μπορούμε να απενεργοποιήσουμε τη χρήση του windows store, όπως ακολούθως:

Ανοίγουμε τον Registry Editor, (με εκτέλεση της regedit, στο πεδίο αναζήτησης) και περιηγούμαστε στο HKLM\Software\Policies\Microsoft\Windows Store

Δημιουργούμε μία νέα μεταβλητή Dword32, με όνομα RemoveWindowsStore και του θέτουμε τιμή 1.

Ρυθμίζοντας την τιμή RemoveWindowsStore σε 0 θα ενεργοποιήσει πάλι το ηλεκτρονικό κατάστημα.



Ρύθμιση του OneDrive

Το OneDrive μας επιτρέπει να διατηρήσουμε τα έγγραφά μας, τις φωτογραφίες μας και τις ρυθμίσεις του υπολογιστή μας στο διαδίκτυο, έτοιμα ώστε να συγχρονιστούν με άλλους σταθμούς εργασίας, στους οποίους εργαζόμαστε. Όμως, τα προσωπικά μας αρχεία είναι αποθηκευμένα στο διαδίκτυο μέχρι κάποιος να παραβιάσει το συνθηματικό μας. Αυτό δεν είναι καθόλου ασφαλές. Εάν έχουμε ρυθμίσει τον υπολογιστή να χρησιμοποιεί έναν Microsoft account, για μεγαλύτερη ασφάλεια ελέγχουμε ότι έχουμε ρυθμίσει το OneDrive, ώστε να μην συγχρονίζει όλα τα έγγραφά και τους ιδιωτικούς μας φακέλους.

Αυτό μπορεί να γίνει ως εξής:

Search -> settings -> OneDrive -> File Storage -> απενεργοποιούμε το 'Save documents to OneDrive by default'

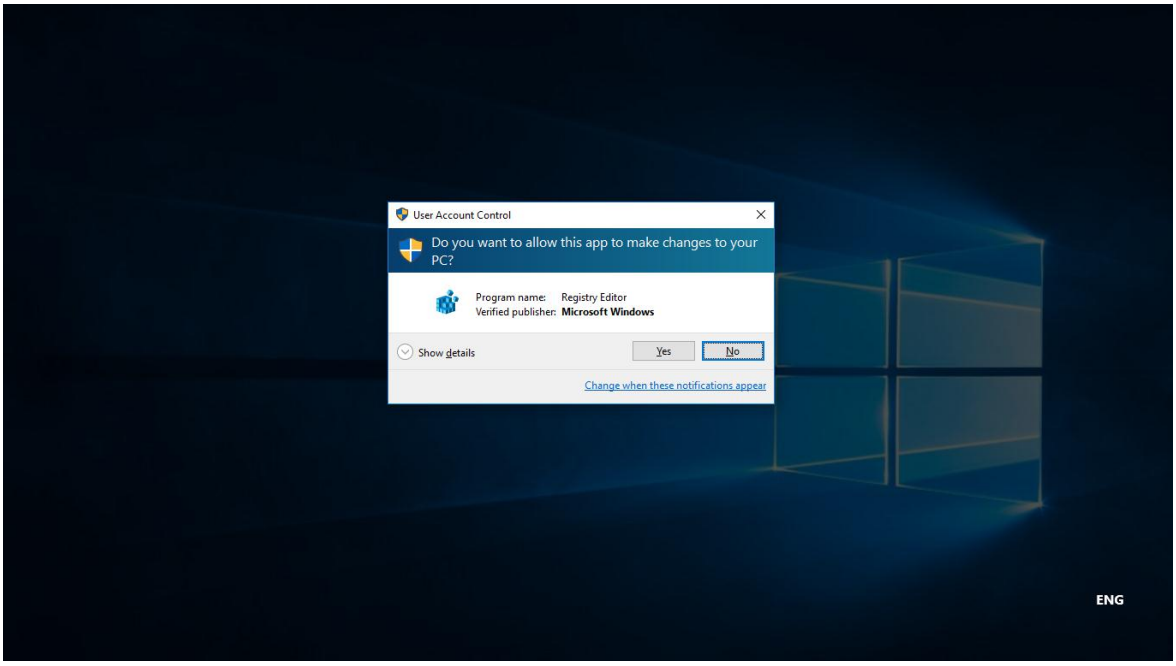
Search -> settings -> OneDrive -> Sync Settings-> απενεργοποιούμε το “Sync your settings on this PC”

Search -> settings -> OneDrive -> Camera roll > επιλέγουμε “Don't upload photos”, και επιπλέον απενεργοποιούμε το 'automatically upload videos to OneDrive'

Τα παραπάνω πρέπει να εφαρμοστούν σε όλους τους MS Accounts.

Ρύθμιση του User Account Control (Ελέγχου Λογαριασμού Χρήστη)

Η λειτουργία **Ελέγχου Λογαριασμού Χρήστη** [User Account Control (UAC)] είναι αυτή η οποία, πριν την εγκατάσταση κάποιου λογισμικού ή το άνοιγμα κάποιων εφαρμογών που ενδεχομένως θα μπορούσαν να βλάψουν τον σταθμό εργασίας, ζητά την άδεια για την εκτέλεσή τους. Ουσιαστικά η λειτουργία αυτή βοηθά στη διατήρηση του ελέγχου του υπολογιστή, παρέχοντας ενημέρωση όταν το πρόγραμμα εφαρμόζει μια αλλαγή για την οποία απαιτούνται δικαιώματα σε επίπεδο διαχειριστή.

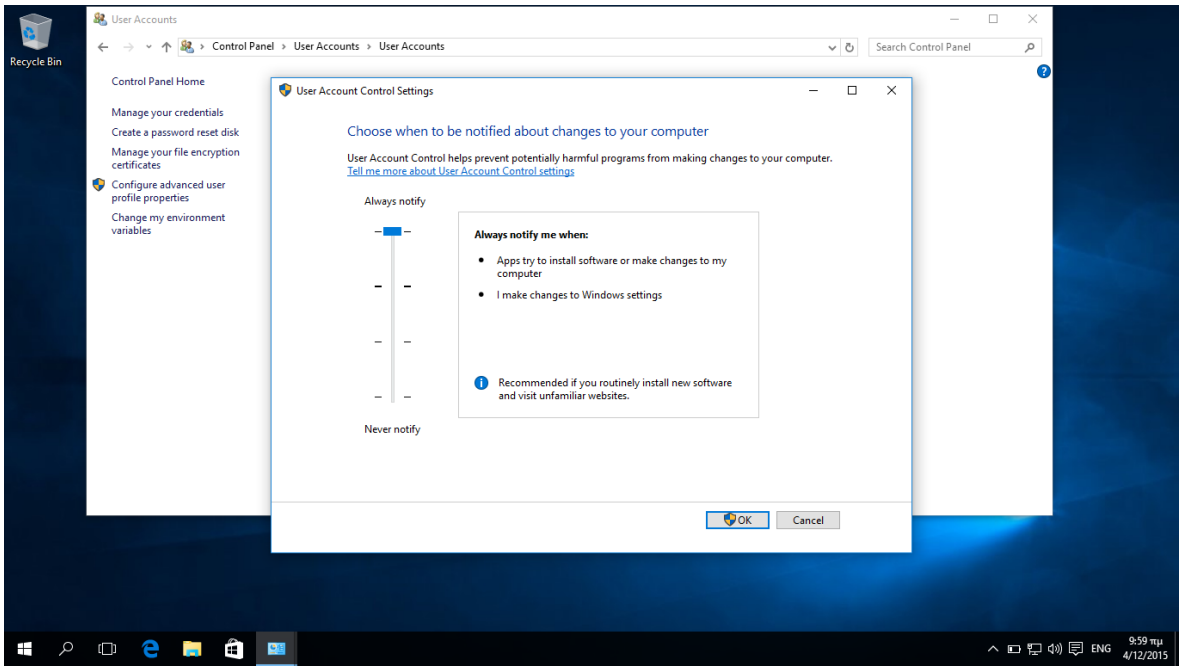


Ρυθμίζουμε το UAC στην μέγιστη τιμή (Turn UAC to the max)

Η Microsoft έκανε έναν συμβιβασμό από τα Windows 7 και επιτρέπει στους χρήστες να επιλέξουν το επίπεδο ελέγχου (level of prompting) που επιθυμούν στο UAC. Για να το επιτύχουμε αυτό, πάμε στο:

Control Panel > All Control Panel Items > User Accounts > Change User Account Control Settings

Τοποθετούμε το δείκτη στην κορυφή.



Προσοχή!

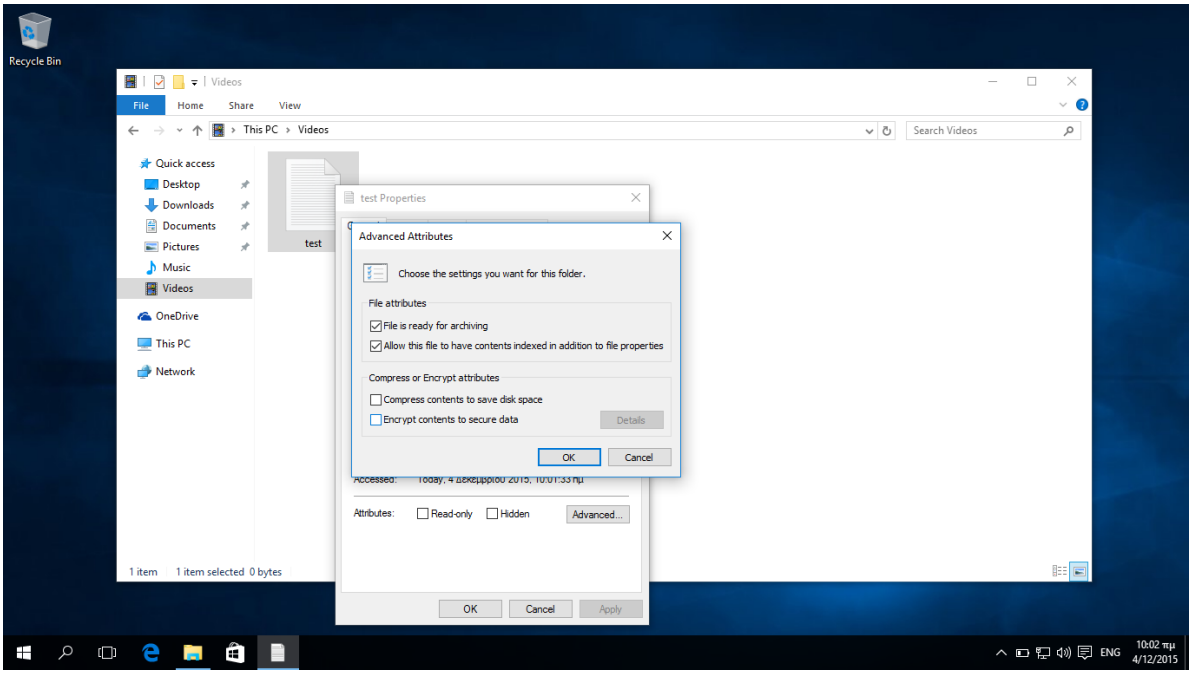
Απενεργοποιώντας το έλεγχο (UAC), σημαίνει απενεργοποίηση της λειτουργίας protected mode του internet explorer.

Κρυπτογράφηση δεδομένων

Για την μέγιστη ασφάλεια των δεδομένων μας, είναι απαραίτητη η κρυπτογράφηση τους, ώστε εάν κλαπεί παράδειγμα το laptop ή ο εξωτερικός σκληρός δίσκος μας, να μην είναι δυνατή, η ανάκτηση των δεδομένων μας από τον κακόβουλο χρήστη.

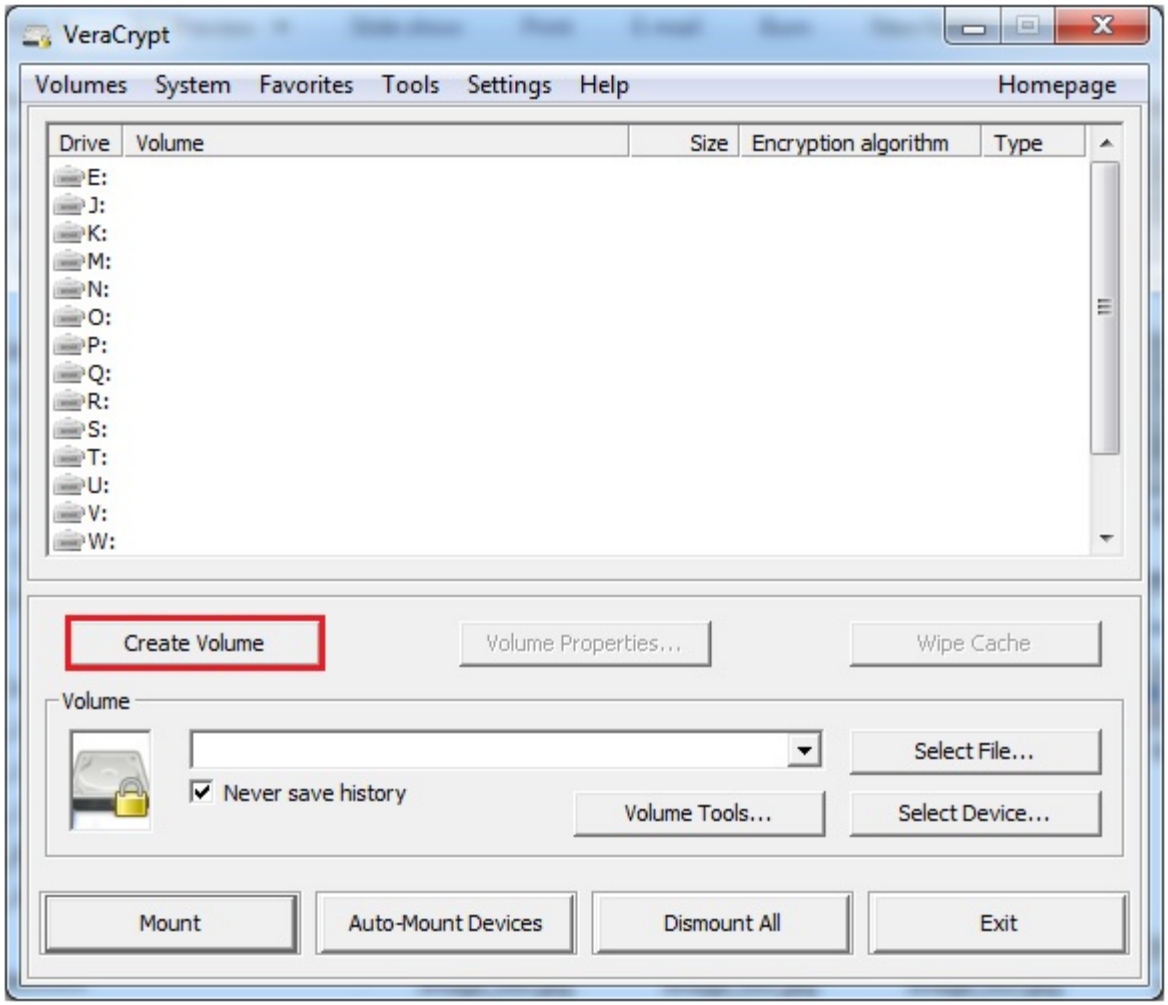
Για να κρυπτογραφήσουμε κάποιο μέσο, είτε ολόκληρο, είτε τμήμα του, υπάρχουν διάφορες εφαρμογές.

Μια ενσωματωμένη λειτουργία στα Windows (από XP και μετά) είναι το EFS (Encrypting File System), με την προϋπόθεση ότι η διαμόρφωση (format) του μέσου είναι σε NTFS. Επιλέγουμε **Start**, **File Explorer**. Βρίσκουμε το αρχείο που θέλουμε να κρυπτογραφήσουμε, κάνουμε δεξί κλικ πάνω του και επιλέγουμε **Properties**. Στην καρτέλα **General**, επιλέγουμε **Advanced**. Κάτω από το **Compress or Encrypt attributes**, επιλέγουμε το **Encrypt contents to secure data** check box και πατάμε **OK**. Αν το αρχείο (file) βρίσκεται σε έναν μη κρυπτογραφημένο φάκελο θα μας ρωτήσει αν θέλουμε να κρυπτογραφήσουμε μόνο το αρχείο ή όλο τον φάκελο. Επιλέγουμε ανάλογα.



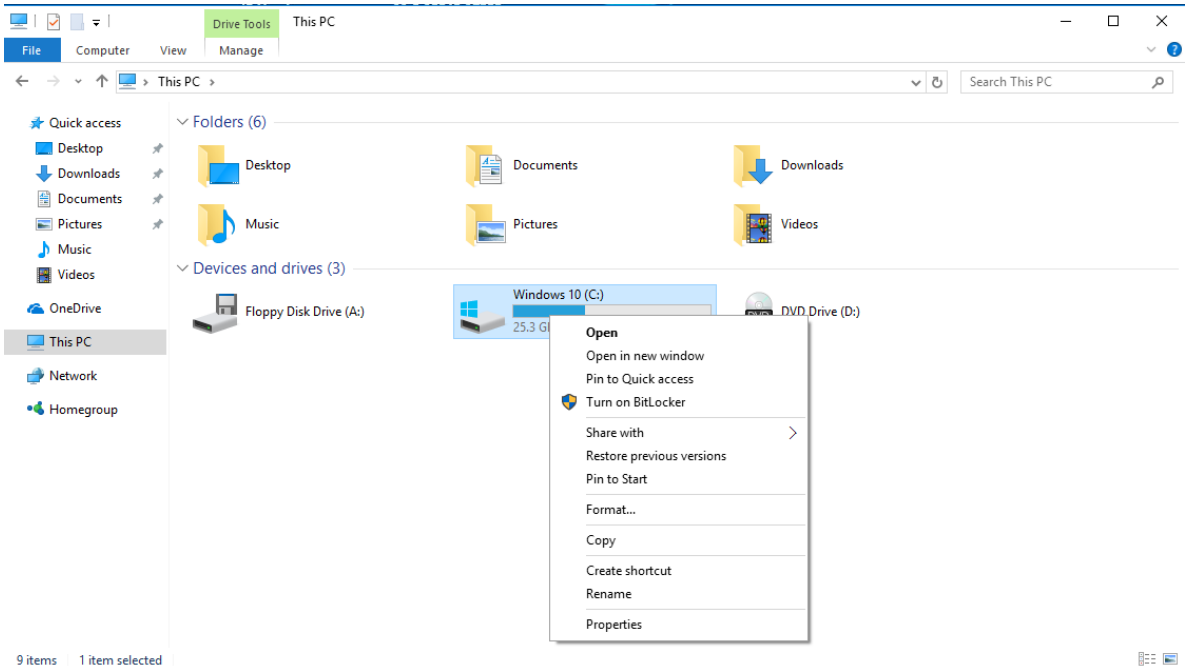
Μια άλλη δωρεάν εφαρμογή είναι το veracrypt. Ένα πλεονέκτημα του veracrypt, είναι ότι μπορούμε να το χρησιμοποιούμε σε διαφορετικά λειτουργικά συστήματα (windows, Linux, MacOs) και έτσι να επεξεργαζόμαστε παντού τα δεδομένα μας.

Αφού εγκαταστήσουμε το veracrypt (https://veracrypt.codeplex.com/), επιλέγουμε **Create Volume** και ξεκινά ο οδηγός veracrypt Volume Creation Wizard. Κάνουμε κλικ στην πρώτη επιλογή **create an encrypted file container**, επιλέγουμε **standard VeraCrypt volume** και πατάμε **NEXT**. Με **Select File** επιλέγουμε που θέλουμε να δημιουργηθεί το container, πώς θα το ονομάσουμε και σώζουμε με **save**. Στη συνέχεια επιλέγουμε τον αλγόριθμο (AES), το μέγεθος του φακέλου, ένα συνθηματικό και αφού το επιβεβαιώσουμε θα ξεκινήσει η διαδικασία της διαμόρφωσης (format). Με το τέλος της διαδικασίας διαμόρφωσης, θα έχει δημιουργηθεί και ο κρυπτογραφημένος τόμος.
Για να τον ανοίξουμε, επιλέγουμε select file > mount και δίνουμε το συνθηματικό μας.



BitLocker Drive Encryption

Πρόκειται για μία εφαρμογή των Windows 10, το οποίο πραγματοποιεί κρυπτογράφηση σε όλο το σκληρό δίσκο. Όταν είναι ενεργό, ολόκληρος ο σκληρός δίσκος είναι κρυπτογραφημένος και δεν θα είναι αναγνώσιμος από άλλες εκδόσεις Windows ή Linux, γεγονός που εμποδίζει τις επιθέσεις με φυσική πρόσβαση.
Για να κρυπτογραφήσουμε έναν σκληρό δίσκο με **BitLocker,** η διαδικασία που ακολουθούμε είναι πολύ απλή. Απλά κάνουμε δεξί κλικ και επιλέγουμε **"Turn on BitLocker".** Παράδειγμα στην εικόνα που ακολουθεί:



Ασφαλής διαγραφή δεδομένων

Η διαδικασία αποστολής δεδομένων στο καλάθι αχρήστων και το άδειασμα αυτού, δεν διαγράφει τα δεδομένα, αλλά διαγράφει τον σύνδεσμο σε αυτά (διαγράφει την εγγραφή στον MFT), ο οποίος μας δείχνει που είναι αποθηκευμένα. Για να διαγράψουμε τα αποθηκευμένα δεδομένα σε έναν δίσκο, θα πρέπει πάνω τους να γράψουμε και να διαγράψουμε τυχαία δεδομένα, τουλάχιστον μία φορά. Μία δωρεάν εφαρμογή που μπορούμε να χρησιμοποιήσουμε είναι το eraser. (http://www.heidi.ie/eraser/download.php).

ΤΜΗΜΑ 7
ΡΥΘΜΙΣΕΙΣ ΣΥΣΤΗΜΑΤΟΣ

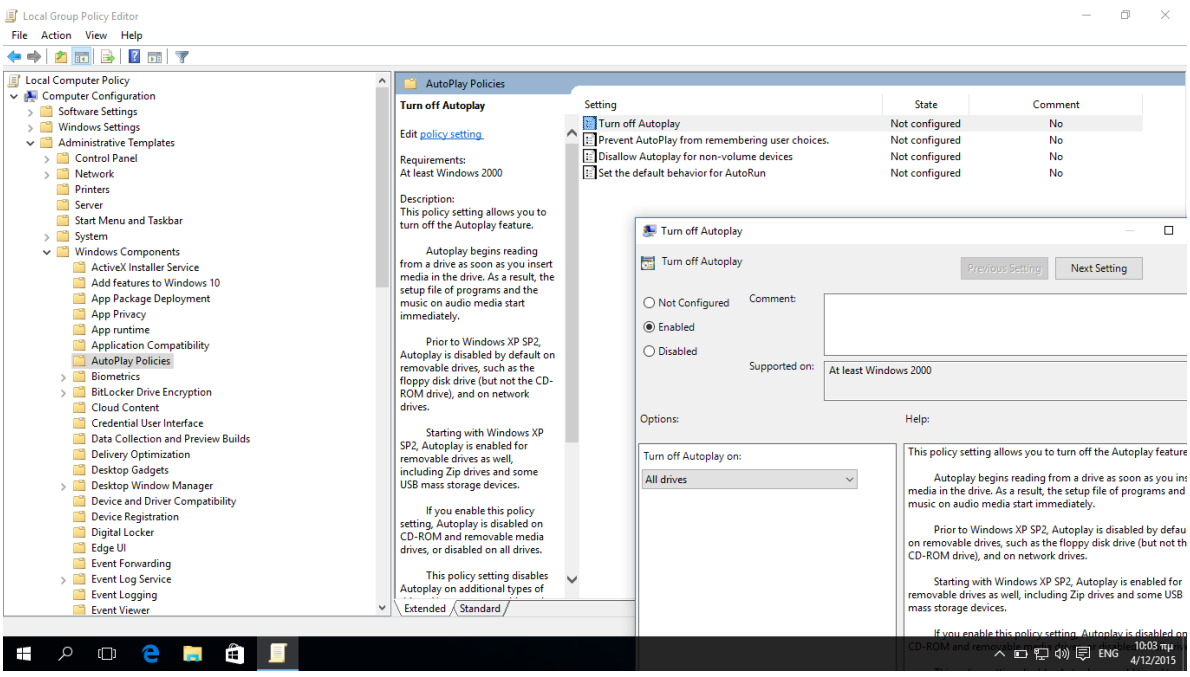
Αυτόματη εκτέλεση (autorun)

Η συγκεκριμένη λειτουργία, παρότι παρέχει διευκολύνσεις στη χρήση διάφορων μέσων (cd, dvd, usb sticks, hards disks), ενέχει πολλούς κινδύνους. Συγκεκριμένα, με την εισαγωγή κάποιου μολυσμένου μέσου, θα γίνει αυτόματη εκτέλεση του ιομορφικού λογισμικού, χωρίς να παρέμβουμε.

Για το λόγο αυτό θα πρέπει να απενεργοποιήσουμε τη συγκεκριμένη λειτουργία όπως παρακάτω:

Στο search , ή πατώντας το windows button (□), στη γραμμή αναζήτησης πληκτρολογούμε gpedit.msc και πατάμε **enter**. Στο Local Computer Policy, επεκτείνουμε το **Computer Configuration**, **Administrative Templates, Windows Components** και στην συνέχεια επιλέγουμε **AutoPlay Policies**.
Στη συνέχεια στο settings panel κάνουμε δεξί κλικ στο **Turn off Autoplay** και επιλέγουμε **Edit**. Στο **Turn off Autoplay** box επιλέγουμε **Enabled** για να απενεργοποιήσουμε το autorun. Βεβαιωνόμαστε ότι στα **Options** είναι προεπιλεγμένο το **All drives** ώστε να εφαρμοστεί σε όλα τα μέσα. Με **OK** κλείνουμε το **Turn off Autoplay Properties** dialog box.

Τέλος, για να εφαρμοστούν οι ρυθμίσεις θα πρέπει να κάνουμε **επανεκκίνηση** στον υπολογιστή. Πλέον, δεν γίνεται αυτόματη εκτέλεση σε καμία συσκευή μας.



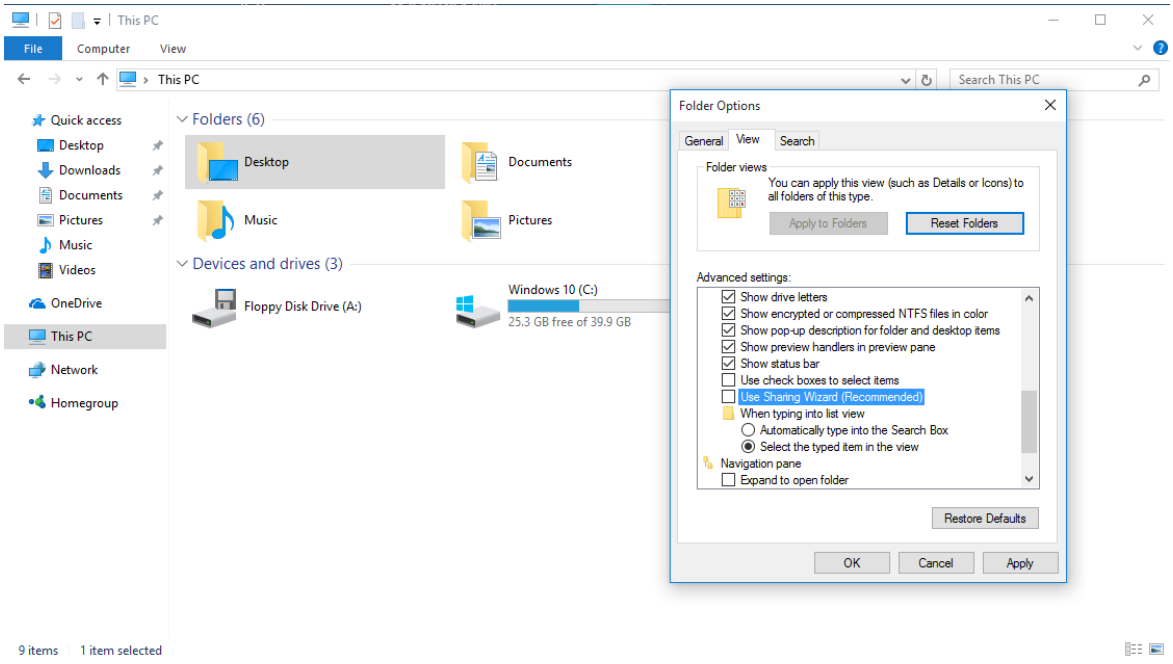
Προσοχή

Εάν διαπιστώσουμε ότι σε κάποια φορητή συσκευή μας εμφανίζεται το αρχείο **autorun.inf**, τότε υπάρχει μεγάλη πιθανότητα αυτή να είναι μολυσμένη με κάποιο ιομορφικό λογισμικό. Το άνοιγμα του αρχείου αυτού με έναν απλό text editor (π.χ. Notepad) θα μας υποδείξει ποιο είναι αυτό το ιομορφικό λογισμικό.

Κοινόχρηστα αρχεία και φάκελοι

Όταν εργαζόμαστε με κοινόχρηστους φακέλους θα πρέπει να χρησιμοποιούμε συνθηματικό και να επιτρέπουμε μόνο την ανάγνωσή τους (read only) και όχι την επεξεργασία των δεδομένων τους. Και αυτό διότι αν δεν έχουμε ρυθμίσει σωστά τον διαμοιρασμό των αρχείων (file sharing), κάποιος κακόβουλος χρήστης με πρόσβαση στο δίκτυο μπορεί να πάρει όλα τα δεδομένα που έχουμε σε αυτόν ή ακόμη και να τοποθετήσει ιομορφικό λογισμικό ώστε να παραπλανήσει το χρήστη να το εκτελέσει. Ωστόσο ο κακόβουλος χρήστης μπορεί να το εκτελέσει και απομακρυσμένα, αφού το τοποθετήσει στον κοινόχρηστο φάκελο (το ιομορφικό λογισμικό) κάνοντας χρήση του scheduler.

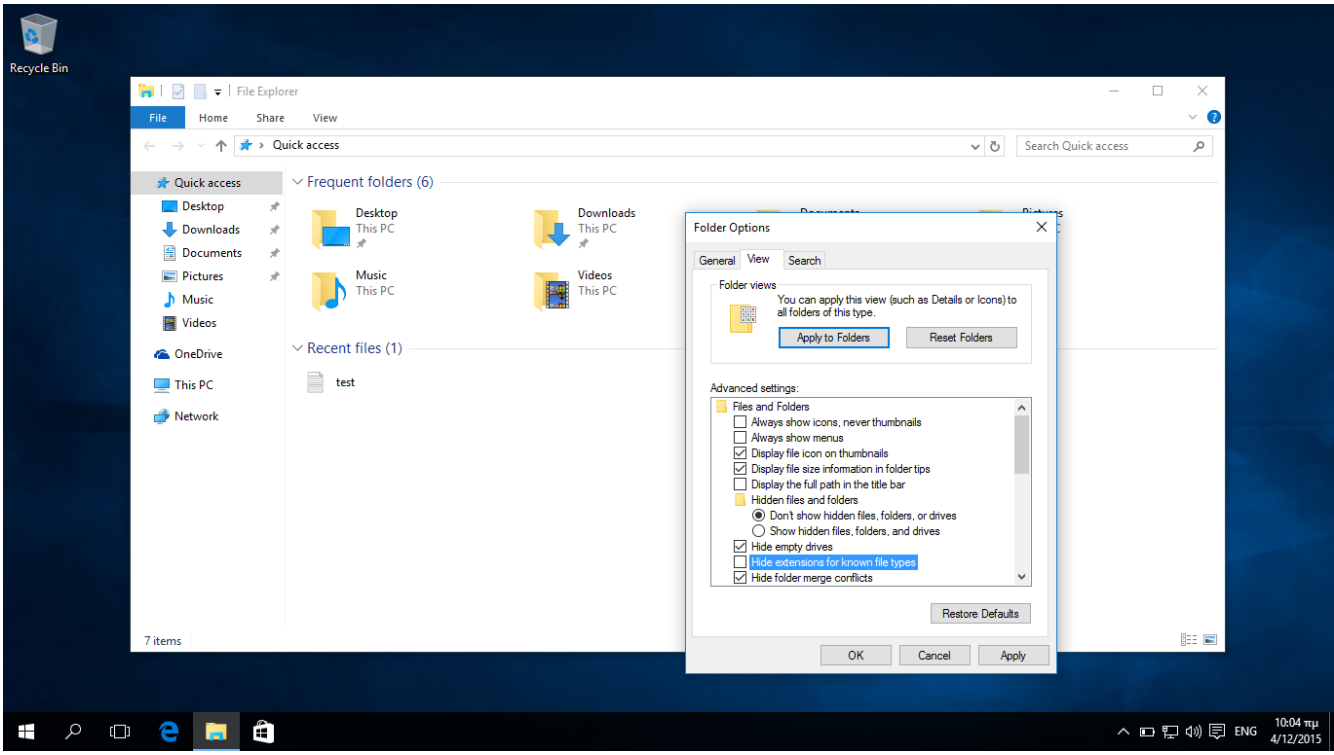
Για να έχουμε **απενεργοποιημένο το file sharing,** η διαδικασία που ακολουθούμε είναι να επιλέξουμε **apps/File Explorer** Στην καρτέλα **View**, στις ρυθμίσεις **Advanced Settings** από-επιλέγουμε το **Use Sharing Wizard (Recommended)** και πατάμε **OK**.



Καταλήξεις αρχείων

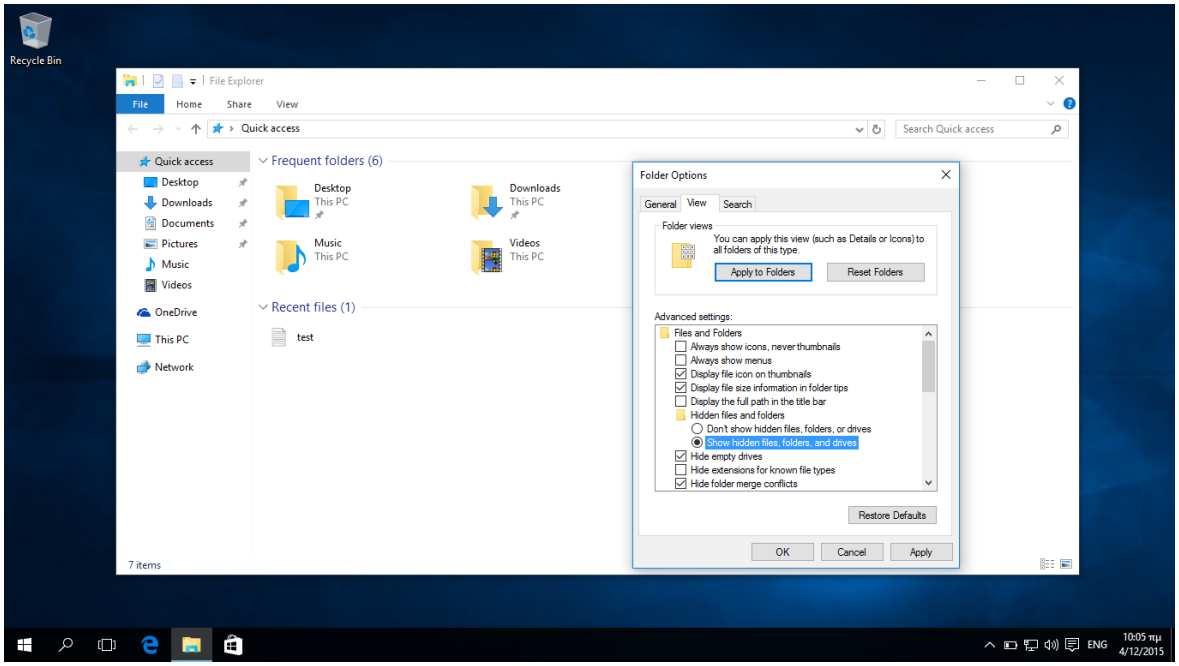
Πολλά ιομορφικά προγράμματα εκμεταλλεύονται την απόκρυψη των καταλήξεων αρχείων που έχει εξ' ορισμού το λειτουργικό σύστημα Windows για να δράσουν. Καλή πρακτική είναι να βλέπουμε όλες τις καταλήξεις όλων των αρχείων. Η διαδικασία που ακολουθούμε είναι να επιλέξουμε το **apps/File Explorer,** στην καρτέλα **View**, στις ρυθμίσεις **Advanced Settings** από-επιλέγουμε το **"Hide**

extensions for known file types" check box και πατάμε **OK** :



Εμφάνιση κρυφών αρχείων

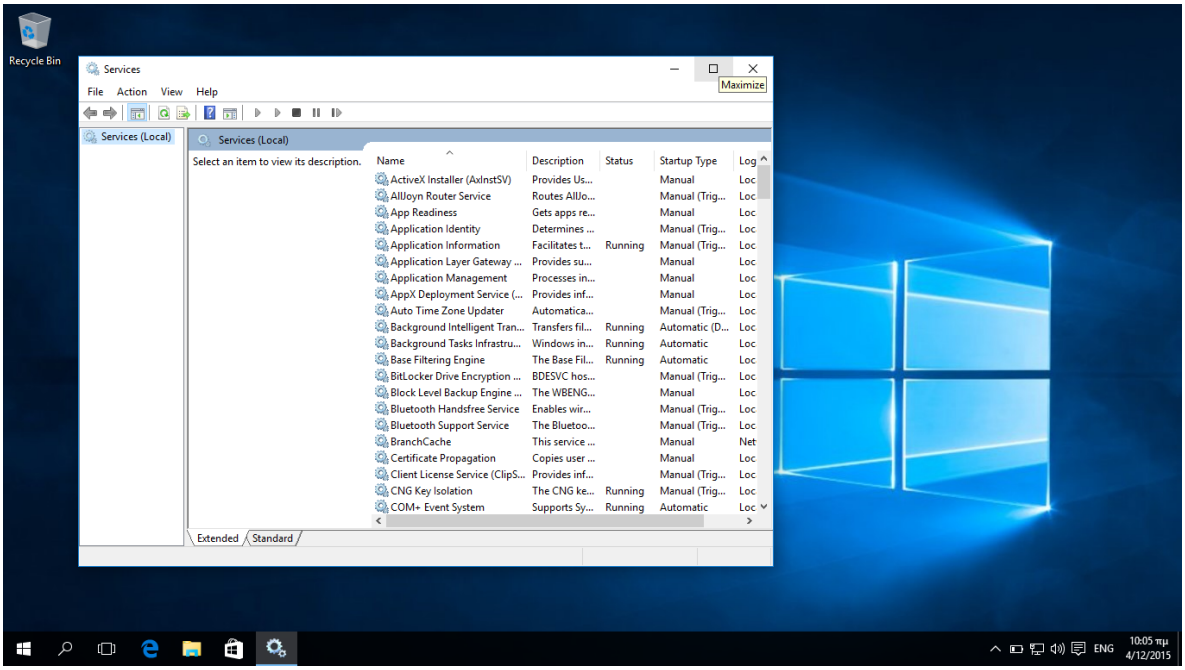
Πολλές επιθέσεις βασίζονται στο γεγονός ότι το λειτουργικό σύστημα Windows αποκρύπτει εξ' ορισμού κάποια αρχεία του συστήματος. Είναι σημαντικό να ρυθμίσουμε τον υπολογιστή μας να εμφανίζει τα κρυφά αρχεία. Η διαδικασία που ακολουθούμε είναι να επιλέξουμε στο μενού **apps/File Explorer** στην καρτέλα **View**, στις ρυθμίσεις : **Advanced Settings** επιλέγουμε το **"Show hidden files, folders and drives"** check box και πατάμε **OK.**



Υπηρεσίες (services)

Είναι σημαντικό να γνωρίζουμε ποιες υπηρεσίες (services) είναι ενεργοποιημένες (εκτελούνται) στον υπολογιστή μας και για ποιο λόγο (πιο σκοπό εξυπηρετούν). Εάν κάποια υπηρεσία είναι ενεργοποιημένη χωρίς να την χρειαζόμαστε, τότε αυτή καταναλώνει πόρους του συστήματος και ενέχει κινδύνους εκμετάλλευσης της. Η διαδικασία που ακολουθούμε για να δούμε ποιες υπηρεσίες εκτελούνται στον υπολογιστή μας είναι η παρακάτω:

Στο search , ή πατώντας το windows button (□), στη γραμμή αναζήτησης πληκτρολογούμε **services.msc** και πατάμε **enter**.
Στην οθόνη εμφανίζεται το παρακάτω παράθυρο :



Σε αυτό μπορούμε να διακρίνουμε ποιες υπηρεσίες έχουν ξεκινήσει (ειναι ενεργοποιημένες). Δεν θα πρέπει να εκτελούνται οι υπηρεσίες telnet, FTP και remote desktop, διότι αυτές μπορούν να χρησιμοποιηθούν κακόβουλα για την εκμετάλλευση του υπολογιστή (δημιουργία back door).

Οι υπηρεσίες του συστήματος που θα πρέπει να είναι απενεργοποιημένες φαίνονται στην παρακάτω λίστα:

Service Name	**Default Startup Type**
Background Intelligent Transfer Service	Manual
Computer Browser	Disabled
IP Helper Service	Disabled
Net.Tcp Port Sharing Service	Disabled
Remote Desktop Configuration	Disabled
Remote Desktop Services	Disabled
Remote Desktop Services UserMode Port Redirector	Disabled
Remote Procedure Call (RPC) Locator	Disabled
Routing and Remote Access	Disabled
Simple Network Management Protocol (SNMP) Trap	Disabled

SSDP Discovery	Disabled
TCP/IP NetBIOS Helper	Disabled
UPnP Device Host	Disabled
WebClient	Disabled
WMI Performance Adapter	Disabled

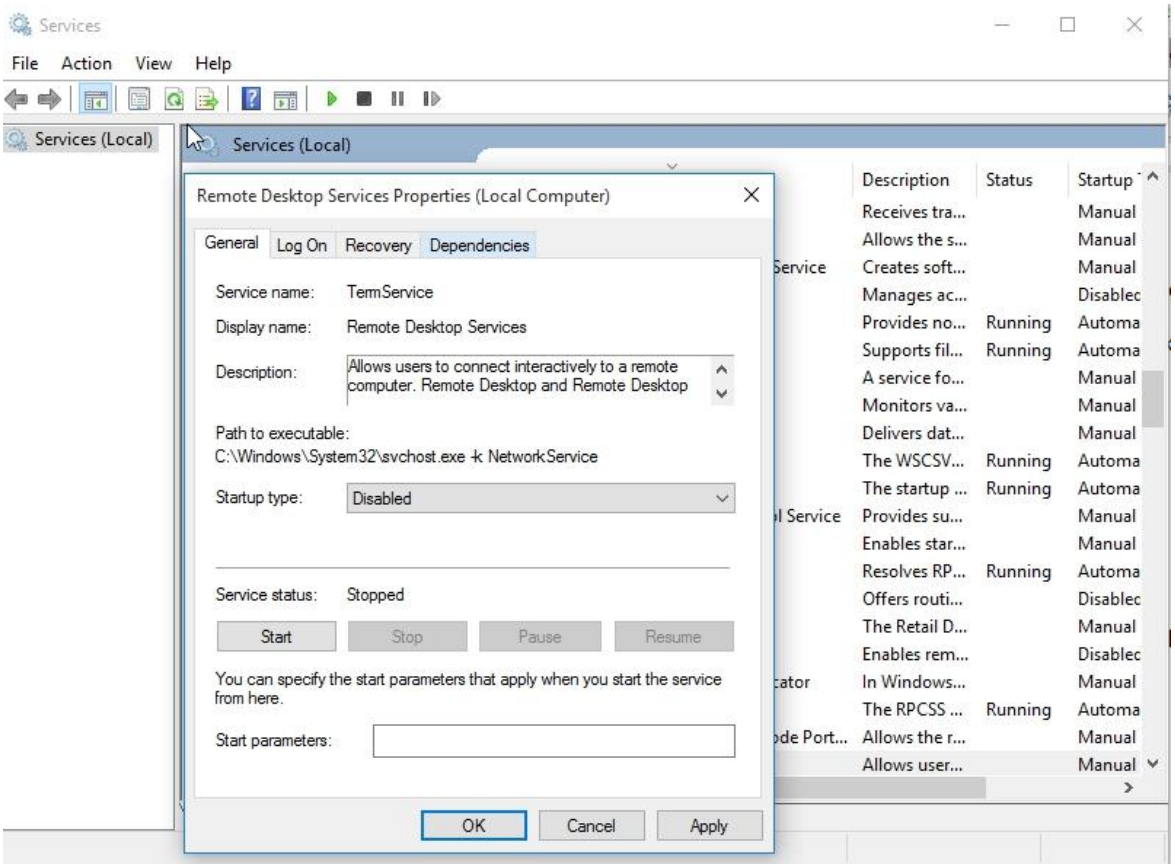
Απενεργοποίηση Ευπαθών Υπηρεσιών

Οτιδήποτε χρησιμοποιεί δεδομένα από το δίκτυο, είναι εύκολο να παραποιηθεί. Πολλοί πιστεύουν ότι οι υπηρεσίες (services) αποτελούν πρόβλημα ασφαλείας, και ότι πρέπει να απενεργοποιούνται. Ενεργοποιημένες πρέπει να παραμένουν μόνο οι υπηρεσίες που χρειάζονται (απαιτούνται για να πραγματοποιήσουμε τις εργασίες μας) . Υπάρχουν πολλές υπηρεσίες, οι οποίες βρίσκονται σε κατάσταση αναμονής, περιμένουν κάποια ενέργεια μέσα από το δίκτυο. Καλή πρακτική είναι αυτές οι υπηρεσίες που δεν μας χρειάζονται να απενεργοποιούνται. Μπορεί στην παρούσα κατάσταση να μην υπάρχει κάποιο γνωστό exploit (εκμετάλλευση αδυναμίας), αλλά γενικότερα για να αποφύγουμε απομακρυσμένες αλληλεπιδράσεις (remote access), μεταξύ των υπηρεσιών, είναι σημαντικό αυτές να απενεργοποιούνται.

Οι υπηρεσίες που θεωρούνται ευπαθείς, φαίνονται στον πίνακα που ακολουθεί και απενεργοποιούνται με τον εξής τρόπο. Πάμε :

Start button >Control Panel > Administrative Tools >Services

Κάνοντας δεξί κλικ , επιλέγουμε Properties και set Startup Type to Disabled.



Παράδειγμα :Disable Remote Desktop Service UserMode Port Redirector

Πίνακας Υπηρεσιών και οι ρυθμίσεις τους που προτείνονται.

Ρύθμιση αυτόματης εκκίνησης (automatic)

Οι παρακάτω υπηρεσίες προτείνεται να είναι ενεργοποιημένες αυτόματα (automatic):

- Distributed link tracking client:(automatic) maintains shortcuts to files on network share if source file is renamed
- DNS client (automatic) only functions as a cache, does not fetch ip addresses
- Infrared monitor service (manual) starts a file transfer automatically when it connects
- IP Helper:(automatic) enables IPv6 tunnels over IPv4. We dont want tunnels; non-inspectable by firewalls.
- Network connected devices auto setup:(manual) devices can still be manually setup

- Remote access auto connection manager:(manual) remote access. not used
- Server:(automatic) disabled because no file printer sharing allowed
- Workstation:(automatic) disabled because no file and print sharing is allowed in network

Οι παρακάτω υπηρεσίες προτείνεται να ενεργοποιούνται χειροκίνητα (manual):

- function discovery provider host: (manual) no need to do network discovery on small lans
- homegroup listener: (manual) dont use homegroup
- homegroup provider: (manual)
- Interactive service detection: (manual) only old services do interaction with desktop. practice not encouraged by MS
- Infrared monitor service (manual) starts a file transfer automatically when it connects
- KTMRM for distributed transaction coordinator (manual) disabled because it is not used.
- Link layer topology discovery mapper: (manual) draws a map of your network. not needed
- NetLogon: (manual) used by domain servers. disabled because no network logons allowed.
- Network connected devices auto setup:(manual) devices can still be manually setup
- Peer name resolution protocol:(manual) disabled because no peers on lan
- Peer networking grouping:(manual) home group. not used
- Peer networking identity manager:(manual) peer to peer networking. not used
- Performance counter DLL host:(manual) allows remote query to performance data

- Phone service: (manual) this is not a phone.

- PNRP machine name publication service:(manual) publishes peer name. disabled because no peers on lan

- Quality windows audio video experience:(manual) QOS. not used

- Remote access auto connection manager:(manual) remote access. not used

- Remote desktop configuration:(manual) remote desktop. not used

- Remote desktop services (manual) remote desktop. Not used

- Remote Desktop Services UserMode Port Redirector (manual) remote desktop. Not used

- Retail demo service:(manual) for demo mode. not used

- Secondary logon:(manual) the runas feature. not used

- Secure socket tunneling protocol service:(manual) disabled because no tunnels to remote points allowed.

- SNMP trap:(manual) disabled because SNMP responds to queries over the network

- SSDP discovery:(manual) disabled because SSDP not allowed

- TCP/IP netbios helper:(manual) disabled because netbios not allowed

- UPnP device host:(manual) disabled becuase no hosting of devices allowed for other pc's

- Webclient:(manual) not used

- Windows Camera Frame Server (manual) enables sending camera video to multiple apps simultaneously, what if for example a spyware app is running in the background.

- Windows media player network sharing service:(manual) disabled because no sharing allowed
- Windows mobile hotspot service:(manual) disabled because no sharing allowed

- Windows remote management:(manual) disabled becuase this

allows remote management

- Work folders:(manual) disabled because no domain servers in standalone config

- Xbox live auth manager:(manual). disabled because no connection to exterior devices allowed

- Xbox live game save:(manual) disabled because no connection to exterior devices allowed

- Xbox live networking service:(manual) disabled because no connection to exterior devices allowed

Οι παρακάτω υπηρεσίες είναι απενεργοποιημένες (disabled) εξ ορισμού:

- Internet connection sharing: (disabled by default)

- Net.Tcp Port sharing service:(disabled by default)

- Remote registry:(disabled by default)

- Routing and remote access:(disabled by default)

- Smart card:(disabled by default)

ΤΜΗΜΑ 8
ΡΥΘΜΙΣΗ ΤΟΥ ΤΕΙΧΟΥΣ ΠΡΟΣΤΑΣΙΑΣ (Firewall)

Ρύθμιση του προφίλ του τείχους προστασίας (Firewall Profile)

Τα Windows λειτουργικά διαθέτουν τρεις (3) δικτυακού τύπους ρυθμίσεις (Profile) στο Firewall που είναι, domain, private και public.

Ιδιωτικό προφίλ (Private): Όταν εργαζόμαστε στο σπίτι βρισκόμαστε στο ιδιωτικό (private) Firewall profile. Αυτό σημαίνει πως είναι ενεργοποιημένο το **network discovery**, έτσι ώστε ο υπολογιστής να μπορεί να επικοινωνήσει με άλλους υπολογιστές στο δίκτυο.

Δημόσιο προφίλ (Public): Οι ρυθμίσεις του δημοσίου προφίλ παρέχουν την περισσότερη ασφάλεια. Μπορεί να χρησιμοποιηθεί σε cafe hotspots, airports κλπ.

Προσοχή:
Εάν το δίκτυο μας περιέχει υπολογιστές που δεν μπορούμε να εμπιστευτούμε τότε ρυθμίζουμε το δικτυακό προφίλ σε δημόσιο.

Το **domain προφίλ** δεν μπορεί να επιλεχθεί από τον απλό χρήστη. Εφαρμόζετε μόνο όταν έχουμε domain.

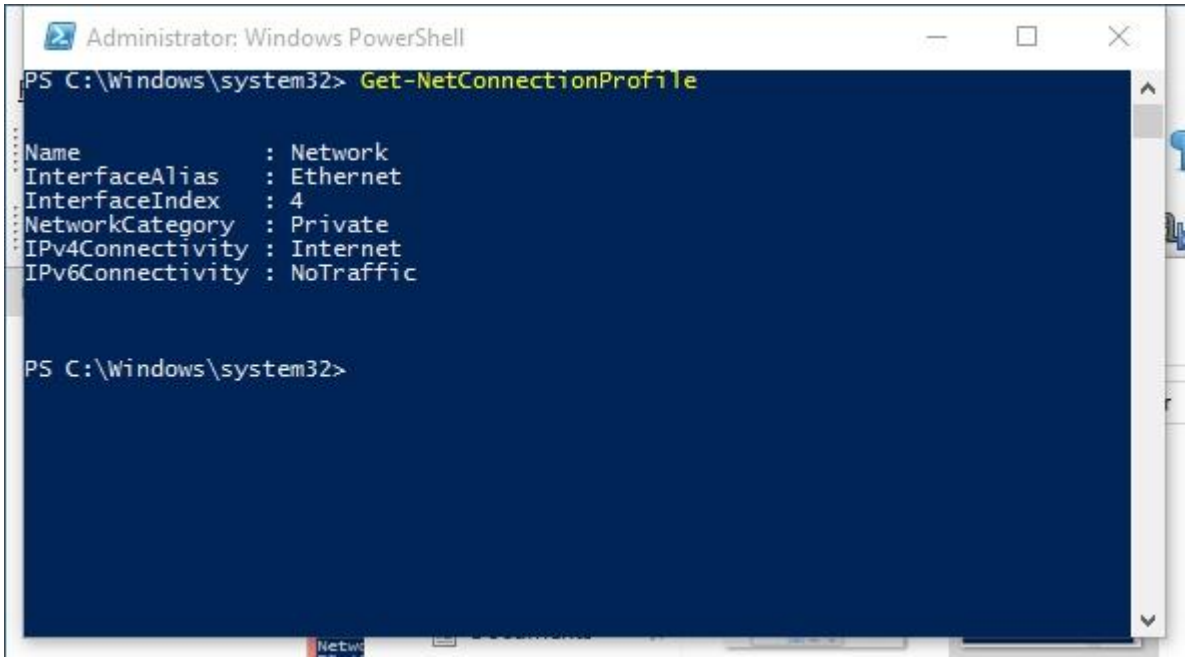
Συνεπώς αν θέλουμε να συνδεθούμε σε domain, επιλέγουμε αυτό το προφίλ (το domain), διαφορετικά επιλέγουμε το δημόσιο για περισσότερη ασφάλεια. Αυτό που επιδιώκουμε είναι να ασφαλίσουμε σωστά τον υπολογιστή μας, θέλουμε την πιο ασφαλή ρύθμιση, όπου θα επιτρέπεται στα Windows να επικοινωνούν, μόνο όταν απαιτείται.

Η επιλογή του τύπου δικτύου (Profile) στις ρυθμίσεις του τοίχους προστασίας (Firewall), γίνεται ως εξής. Επιλέγουμε (Ακολουθούμε την διαδρομή) :

Control Panel > Network and Sharing Center και επιλέγουμε **public**.

Εάν έχουμε επιλέξει private σε Windows 10, η μόνη λύση για να αλλάξει είναι μέσω PowerShell : ΔΕΞΙ κλικ PowerShell -> Run as administrator και πληκτρολογούμε :

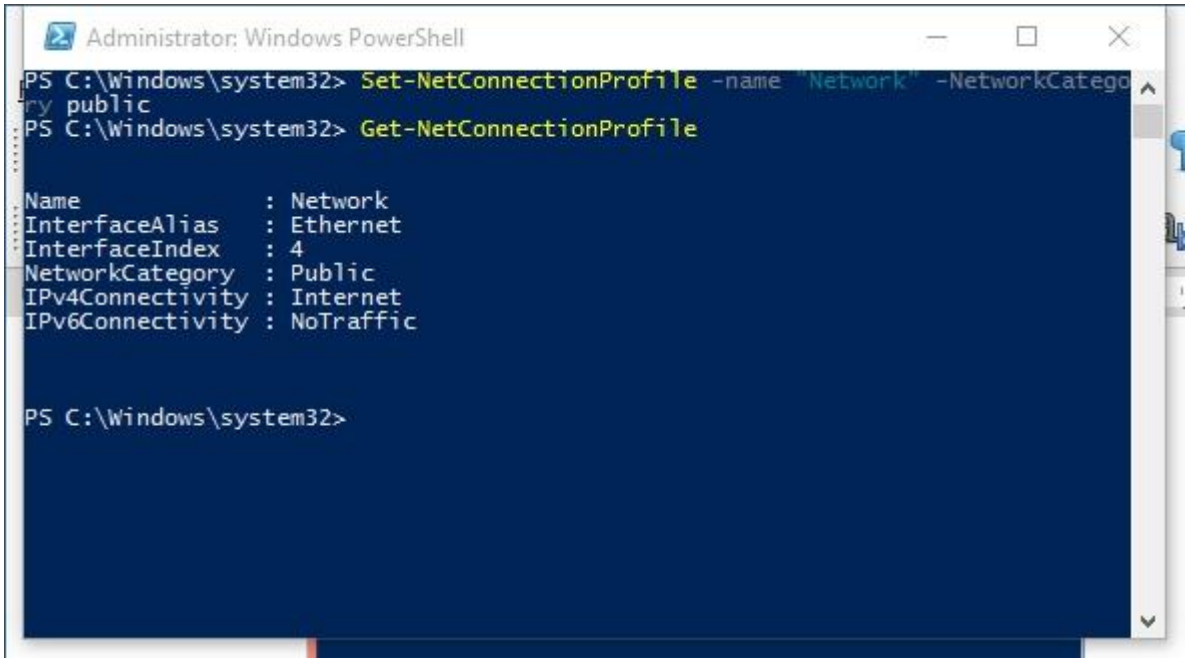
Get-NetConnectionProfile



Διακρίνουμε ότι είναι ρυθμισμένο στο private. Για να το αλλάξουμε σε public πληκτρολογούμε την παρακάτω εντολή:

PS c:\> Set-NetConnectionProfile -name "Network" -NetworkCategory public

Παρατηρούμε ότι αλλάζει σε public.



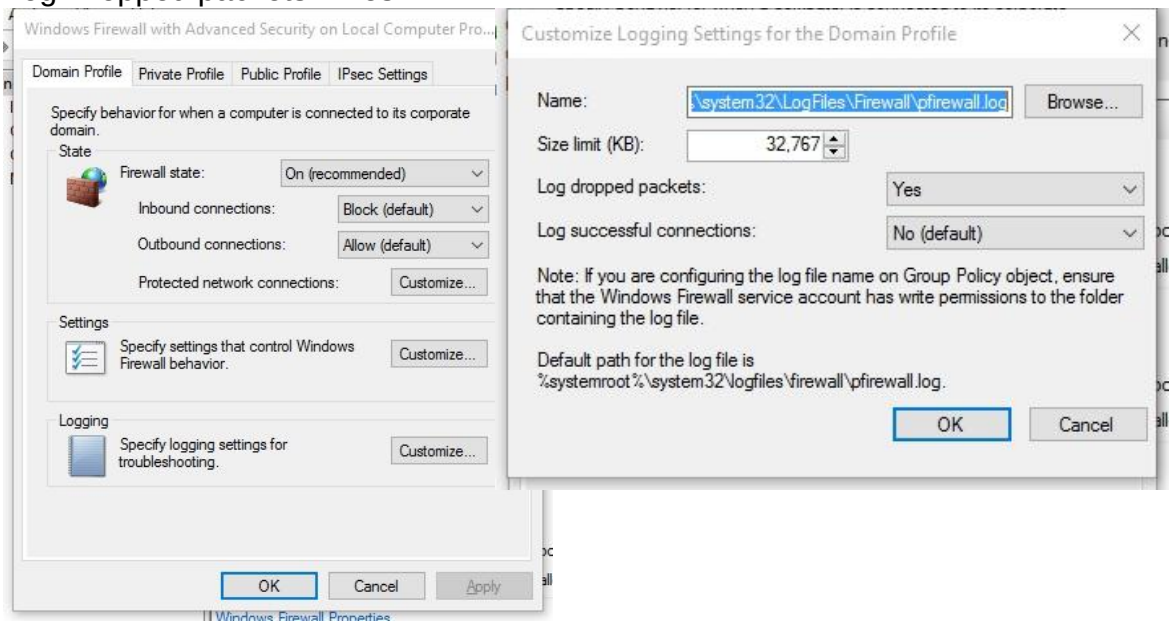
Ρυθμίσεις του τοίχους προστασίας για προχωρημένους (Windows Advanced Firewall), turn on outbound blocking and logging

Η βασική αρχή παραμετροποίησης των firewalls είναι '**default deny**'. Αυτό σημαίνει ότι όλη η κίνηση εμποδίζεται, εκτός εάν έχουμε δημιουργήσει ένα κανόνα που να την επιτρέπει. Αυτοί οι κανόνες είναι γνωστοί ως 'whitelist' γνωστών εφαρμογών και πρωτοκόλλων. Η εξ ορισμού πολιτική (default policy) των Window's firewall's ρυθμίζεται σε inbound deny και outbound allow all, που σημαίνει δεν επιτρέπεται η εισερχόμενη κίνηση δεδομένων και επιτρέπεται όλη η εξερχόμενη. Η ρύθμιση "Outbound allow all" δεν ακολουθεί την αρχή 'default deny'. Δεν επιθυμούμε και δεν επιτρέπουμε το ιομορφικό λογισμικό (malware backdoor) να μπορεί να καλέσει 'πίσω' στους servers του. Με λίγα λόγια δεν επιτρέπουμε την αντίστροφη σύνδεση (reverse connection) μιας backdoor με τους command and control servers του.

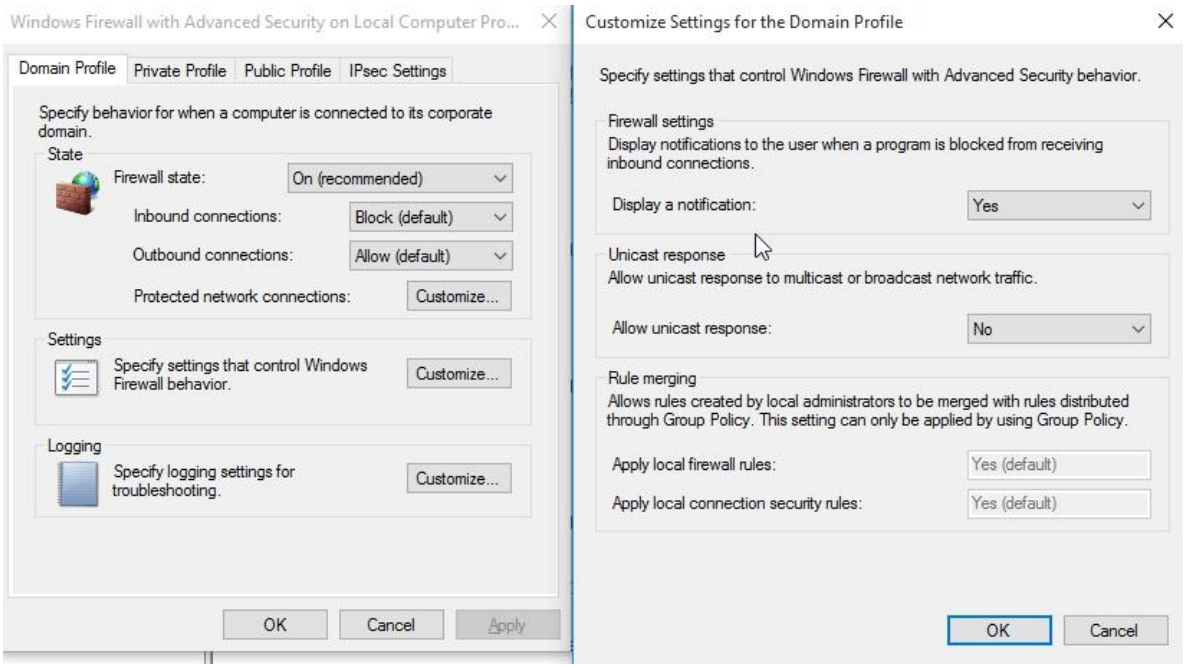
Μπορούμε να θέσουμε το outbound blocking on, να εμποδίσουμε όλη την εξερχόμενη κίνηση δεδομένων και να δημιουργήσουμε κανόνες. Όταν θέτουμε outbound blocking on, επιτρέπει μόνο στα προγράμματα και στις υπηρεσίες που ορίζουμε εμείς, να επικοινωνούν στο διαδίκτυο. Για να το επιτύχουμε αυτό, ενεργούμε ως εξής:

Πάμε στο
Control Panel > Administrative Tools > Windows Firewall with Advanced Security > "Windows Firewall Properties" link :
Όπου εδώ κάνουμε τις εξής ρυθμίσεις :
Θέτουμε **Outbound connection = Block**
Αυξάνουμε το μέγεθος του μητρώου καταγραφής (log file) επιλέγοντας -->
Specify Logging settings for Troubleshooting > Customize

Size Limit = 32767 KB (το οποίο είναι η μέγιστη επιτρεπόμενη τιμή)
Log Dropped packets = Yes



Specify Settings that control Windows Firewall Behavior > Customize
Allow Unicast Response: No



<u>Κανόνες του τοίχους προστασίας (Firewall Rules)</u>
Ένα παράδειγμα κανόνα που επιτρέπουμε μία υπηρεσία να έχει εξερχόμενη επικοινωνία (windows service outbound):

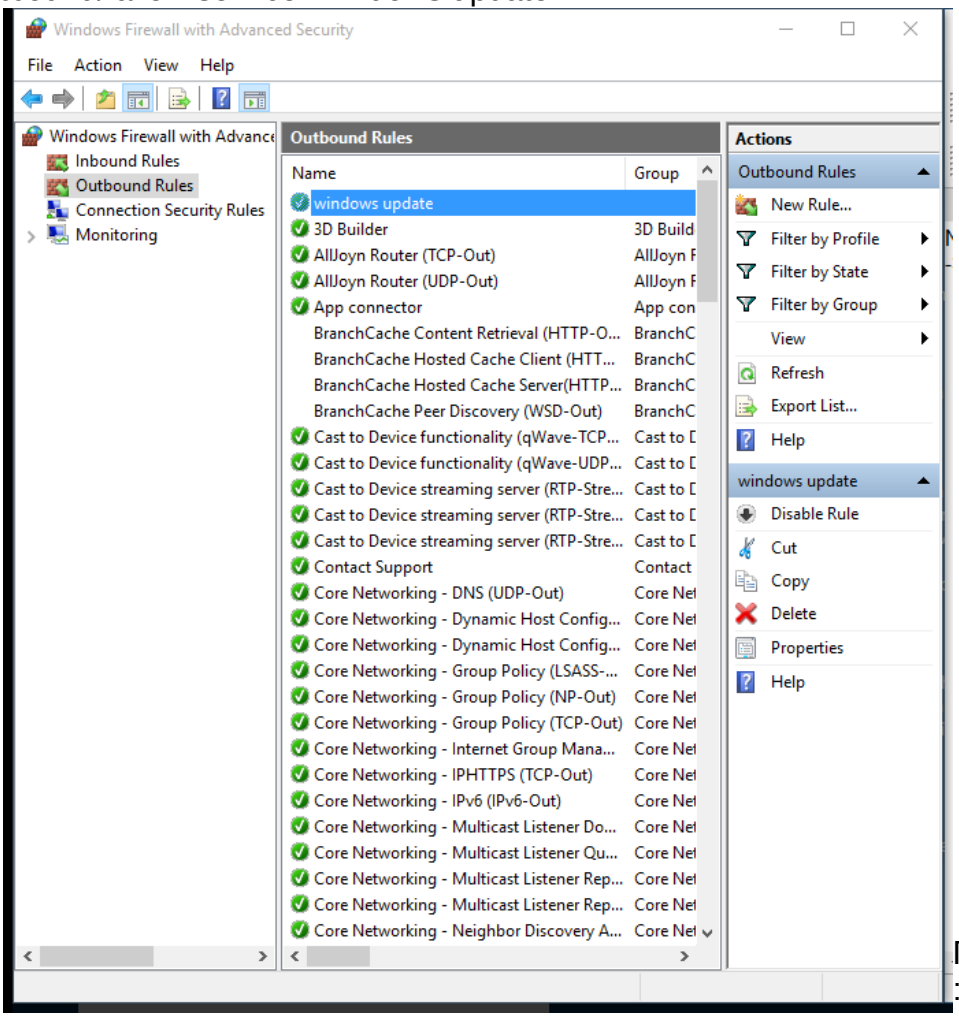
Κλικ στο Outbound Rules στα αριστερά, κλικ στο 'New Rule', επιλέγουμε 'Custom', στη συνέχεια στα 'Services' επιλέγουμε customize, επιλέγουμε 'Apply to this service', βρίσκουμε το 'Windows Update', στη συνέχεια ports and protocol - (καμία αλλαγή), μετά IP addresses (καμία αλλαγή), επιλέγουμε 'Allow The Connection'. Δίπλα επιλέγουμε όλα τα profiles. Τέλος δίνουμε στον κανόνα ένα όνομα.

Ένα παράδειγμα κανόνα που επιτρέπουμε ένα πρόγραμμα να έχει εξερχόμενη επικοινωνία (outbound):

Κλικ στο Outbound Rules στα αριστερά, κλικ στο 'New Rule', επιλέγουμε "Program", επιλέγουμε "This program Path" και πατάμε το "Browse" button, περιηγούμαστε στο φάκελο του προγράμματος και επιλέγουμε το .exe αρχείο, στη συνέχεια επιλέγουμε "Allow the connection", επιλέγουμε όλα τα profiles. Τέλος δίνουμε ένα όνομα στο κανόνα που μόλις δημιουργήσαμε.

Οι ακόλουθοι κανόνες εφαρμόζονται σε όλα τα profiles: Domain, Private and Public

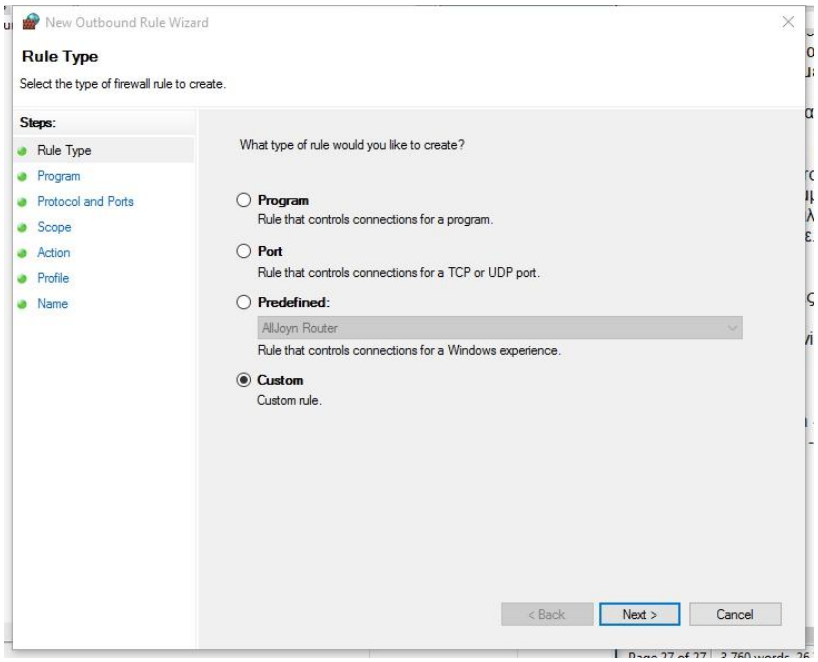
Outbound/ allow service 'Windows update'

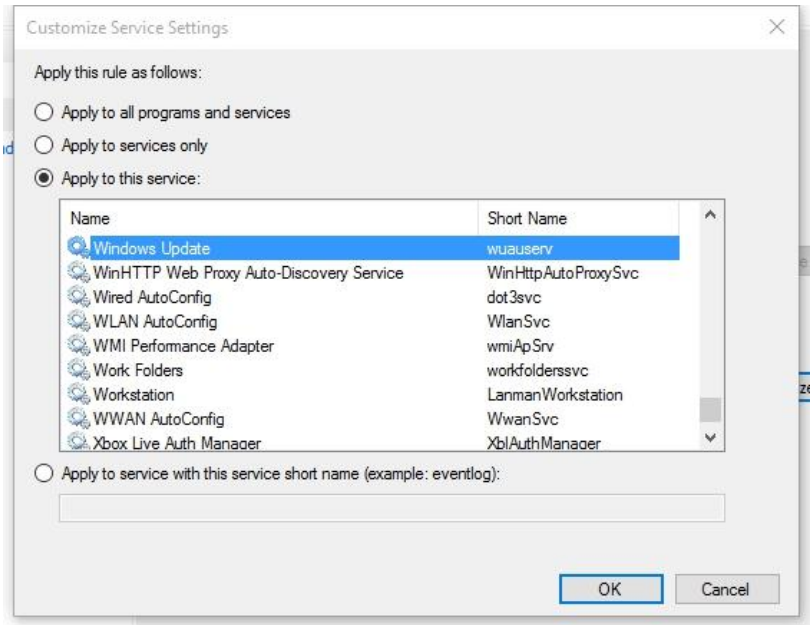


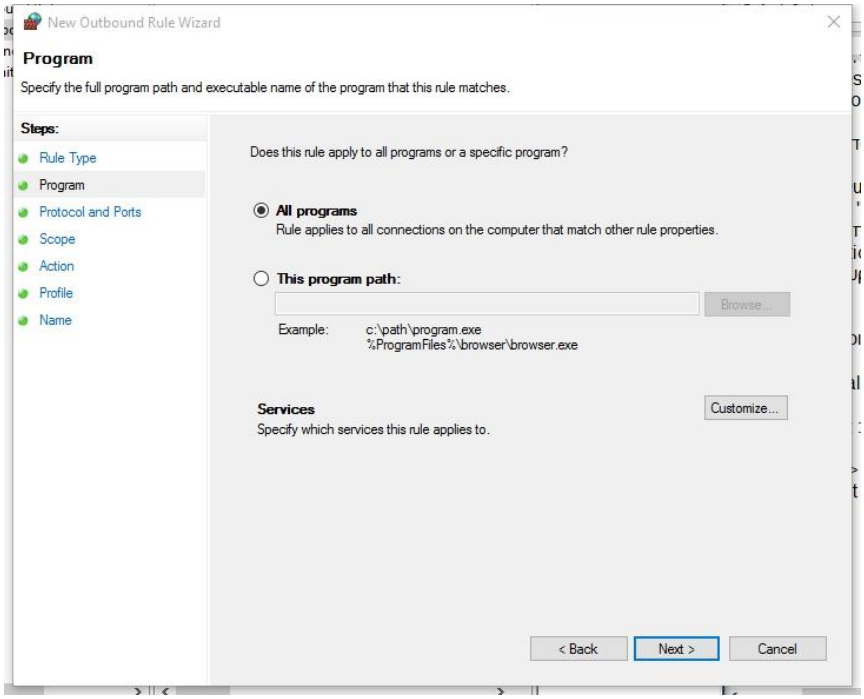
Παράδειγμα:

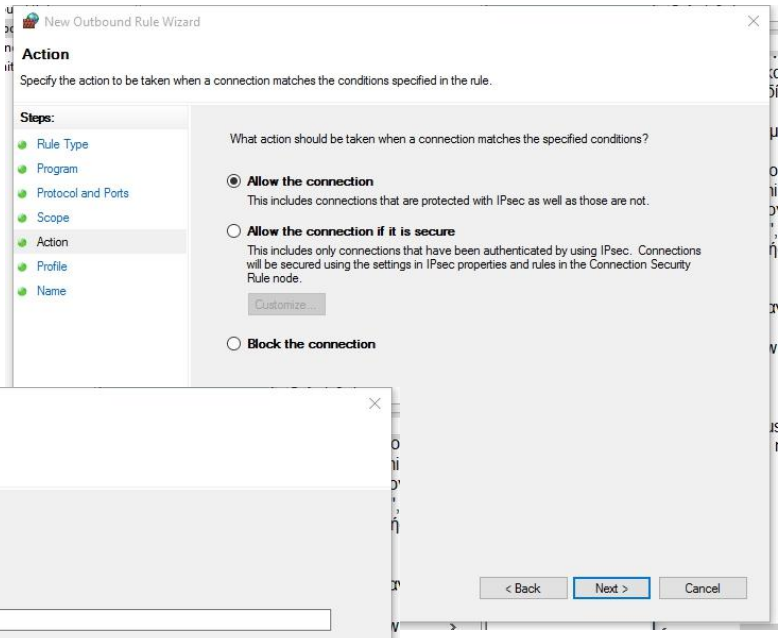
New Rule -> custom -> next -> customize -> apply to this service -> ex. Windows

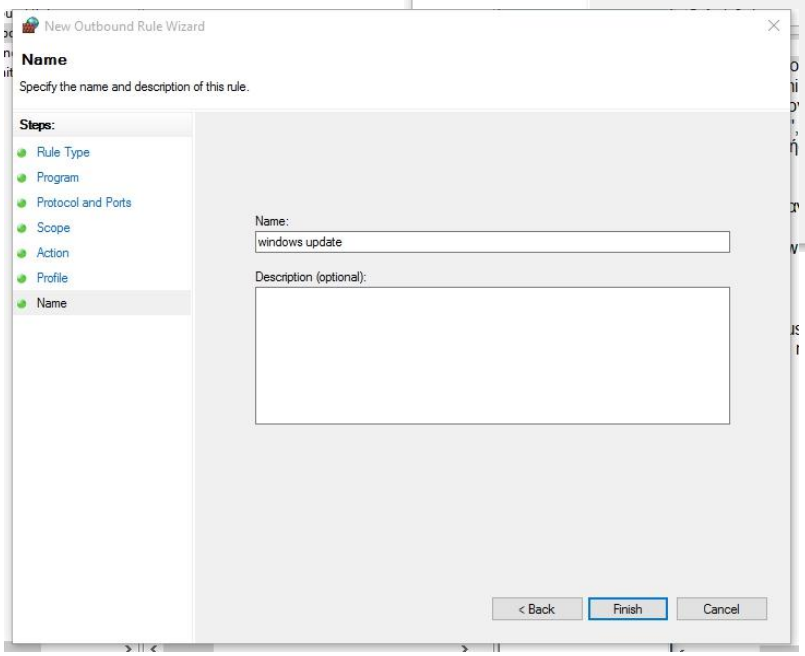
update -> ok -> next -> next -> next -> allow this connection -> next -> next ->name

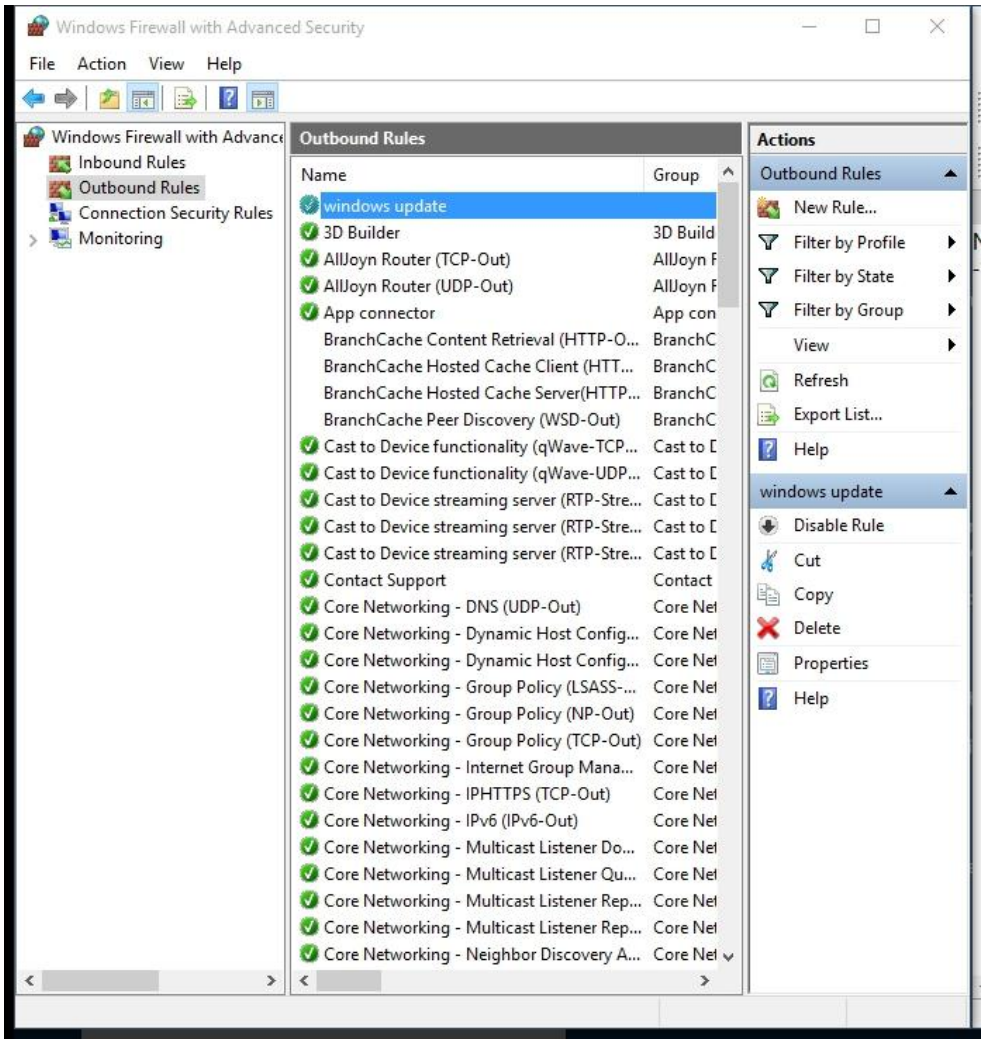





New Outbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
Cancel


New Outbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


New Outbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
windows update
Description (optional):
< Back
Finish
Cancel



Ακολουθώντας τα παραπάνω βήματα, δημιουργούμε ένα κανόνα για όποια υπηρεσία (service) επιθυμούμε. Αντίστοιχα, ακολουθώντας τα βήματα που αναφέρθηκαν στην αρχή, δημιουργούμε ένα κανόνα για όποιο πρόγραμμα ή Ηλεκτρονική Διεύθυνση (IP address) ή πόρτα επιθυμούμε.
Οι προτεινόμενοι κανόνες είναι οι ακόλουθοι:

- Outbound/ allow service 'Windows update'
- Outbound/ allow service 'Windows Time'
- Outbound/ allow program "\Windows\explorer.exe" (SmartScreen Filter)
- Outbound/ allow program '\Windows\HelpPane.exe' (Windows Help, enables fetching online help)
- Outbound/ allow program '\program files\windows defender\MpCmdRun.exe"

- Outbound/ allow program <Firefox/Chrome/Opera, whichever browser you use>
- Outbound/ allow program \program files\Internet explorer\iexplore.exe
- Outbound/ allow program \program files x86\Internet explorer\iexplore.exe
- Outbound/ allow program\Windows\ImmersiveControlPanel\SystemSettings.exe
- Outbound/ allow program \windows\system32\UserAccountBroker.exe
- Outbound/ allow program <your antivirus update program>
- Outbound/ allow program “%ProgramFiles% (x86)\Secunia\PSI\psia.exe
- Outbound/ allow program “%ProgramFiles% (x86)\Secunia\PSI\psi.exe
- Outbound/ allow program \windows\system32\wwahost.exe
- Outbound/ allow program \windows\system32\AuthHost.exe
- Outbound/ allow program \windows\system32\RunTimeBroker.exe
- Outbound/ allow program '\Program files\Windows Media Player\wmplayer.exe
- Outbound/ allow program '\Program files (x86)\Windows Media Player\wmplayer.exe
- Outbound/ allow program <Adobe Flash Update service>
- Outbound/ allow program <Adobe Acrobat Update service>
- Outbound/ allow program \windows\system32\svchost.exe
- Για το SVCHOST, θα πρέπει να δημιουργήσουμε δύο κανόνες:
  Πρώτος κανόνας: πρόγραμμα--> \windows\system32\svchost.exe. Το ονομάζουμε "SCVHOST UDP 53". Επιλέγουμε τον κανόνα και επιλέγουμε ιδιότητες (Properties). Πάμε στην καρτέλα πρωτοκόλλου και πόρτας και ρυθμίζουμε ως πρωτόκολλο 'UDP' set Protocol Type='UDP', ρυθμίζουμε ως απομακρυσμένη πόρτα την 53 (Remote ports to Specific Ports, and type in '53').
  Δεύτερος κανόνας: πρόγραμμα --> \windows\system32\svchost.exe. Το ονομάζουμε "SVCHOST TCP 80,443' Επιλέγουμε τον κανόνα και επιλέγουμε ιδιότητες (Properties). Πάμε στην καρτέλα πρωτοκόλλου και πόρτας και ρυθμίζουμε ως πρωτόκολλο 'TCP' (set Protocol Type='TCP'), ρυθμίζουμε ως απομακρυσμένη πόρτα την 80,443 (set Remote ports to Specific Posts, and type in '80,443').

- Outbound/ allow program \windows\system32\wermgr.exe
- Outbound/ allow program< \users\<userAccountName>\appdata\local\microsoft\onedrive\onedrive.exe> (if you choose to use OnrDrive, each account that uses OneDrive needs a rule)
- Outbound/ allow Core Networking DHCP-out
- Outbound/ disable all Core Networking rules that mentions IPv6, IPHTTPS, IGMP, Teredo, and ICMPv6
- Outbound/ disable the 2 rules that mentions HomeGroup
- Outbound/ disable all rules for Remote Assistance
- Outbound/ disable Proximity Sharing over TCP
- Outbound/ disable all Network Discovery rules
- OutBound/ disable <Mail> (Disable if you don't have MS accounts)
- OutBound/ disable <Calendar and People> (Disable if you don't have MS accounts)
- OutBound/ disable Microsoft Phone Companion (should be for smartphone platforms only)
- OutBound/ disable Message Queuing TCP Outbound
- OutBound/ disable Message Queuing UDP Outbound
- InBound/ allow <Core Networking ICMPv4 in> (enable this rule if you want to be able to ping your machine)
- InBound/ allow Core Networking DHCP in
- Inbound/ allow program <Mcafee Site Advisordir>siteadv.exe
- Inbound/ allow service <SA Service> (Mcafee site advisor)
- InBound/ disable Core Networking IPHTTPS in
- InBound/ disable Core Networking IGMP in
- InBound/ disable all Core Networking rules that mentions IPv6, Teredo, and ICMPv6

- InBound/ disable all Network Discovery rules for private profile (NB Datagram in, NB Name in, LLMNR UDP In, Pub-WSD-In, SSDP-In, UPnP-In, WSD-Events-In, WSD-EventsSecure-In, WSD-In)

- InBound/ disable the 2 rules that mentions HomeGroup

- InBound/ disable DIAL protocol server x2 (allows remote control of apps)

- InBound/ disable Microsfot Edge (it is a browser, only outgoing needed, no unsolicted traffic allowed)

- InBound/ disable Message Queuing x2

- InBound/ disable Proximity Sharing over TCP

- InBound/ disable Search (dont know why search needs a inbound rule, search reaches outbound)

- InBound/ disable Proximity Sharing over Tcp

- InBound/ disable all rules for Remote Assistance

- InBound/ disable <Mail and Calendar> (Disable if you don't use MS accounts)

- InBound/ disable <People> (Disable if you don't use MS accounts)

Ρύθμιση χρήσης μόνο των απαραίτητων πρωτοκόλλων δικτύου (Use only Bare Essential Network protocols)

Στο πλαίσιο μείωσης της επιθετικής επιφάνειας, θα πρέπει να ρυθμίσουμε τον υπολογιστή μας να έχει ενεργοποιημένα μόνο τα πρωτόκολλα που χρειαζόμαστε. Ένας κακόβουλος χρήστης για να έχει την δυνατότητα να πάρει πρόσβαση στον υπολογιστή μας, χρειάζεται να αλληλεπιδρά με κάποιο πρόγραμμα/ πρωτόκολλο που είναι ενεργοποιημένο στον υπολογιστή μας. Επίσης χρησιμοποιεί πρωτόκολλα δικτύου προκειμένου να επικοινωνήσει με άλλους υπολογιστές, συνδεδεμένους στο δίκτυο όπου κάθε ένας από αυτούς μπορεί να έχει αδυναμίες. Συνεπώς, είναι καλό να απενεργοποιούμε τα πρωτόκολλα που δεν χρησιμοποιούνται και να επιτρέπουμε μόνο τα απολύτως απαραίτητα. Πολλά πρωτόκολλα σε χρήση σημαίνει μεγαλύτερη επιφάνεια επίθεσης.

Το μοναδικό πρωτόκολλο που χρειαζόμαστε είναι το IPv4. Το μεγαλύτερο μέρος δικτυακού εξοπλισμού απαιτεί το IPv4, ώστε να λειτουργήσει.

Το NetBIOS over TCP/IP δεν απαιτείται, διότι το NetBIOS είναι ήδη ενεργό χωρίς αυτή την επιλογή. Απενεργοποιώντας το NetBIOS over TCP/IP, περιορίζεται η κίνηση στο τοπικό υποδίκτυο (subnet).

Τα Discovery protocols χρησιμοποιούνται για να παρέχουν μια εικόνα του δικτύου. Για τους οικιακούς χρήστες δεν χρειάζονται τα Discovery protocols, αφού υπάρχει μόνο ένας router.

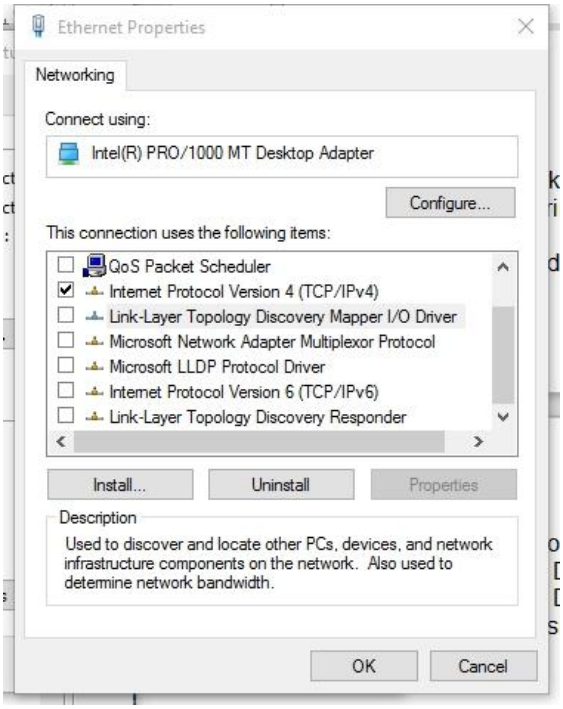
Η επιλογή File and Printer Sharing δεν χρειάζεται να είναι ενεργοποιημένη, εκτός και αν θέλουμε να μοιραστούμε κάποιους φακέλους στο δίκτυο. Σε περίπτωση που επιθυμούμε να εκτυπώσουμε κάτι, είναι καλύτερο να χρησιμοποιούμε έναν εκτυπωτή, ο οποίος είναι δικτυακός (έχει networking built in), έτσι ώστε όταν δεχόμαστε επίθεση, οι επιτιθέμενοι να πάρουν πρόσβαση μόνο στον εκτυπωτή και όχι στον υπολογιστή μας. Απενεργοποιούμε αυτό το χαρακτηριστικό. Ακολουθούμε τα παρακάτω βήματα, πάμε στο:

Control Panel > Network and Sharing Center > Change Adapter Settings

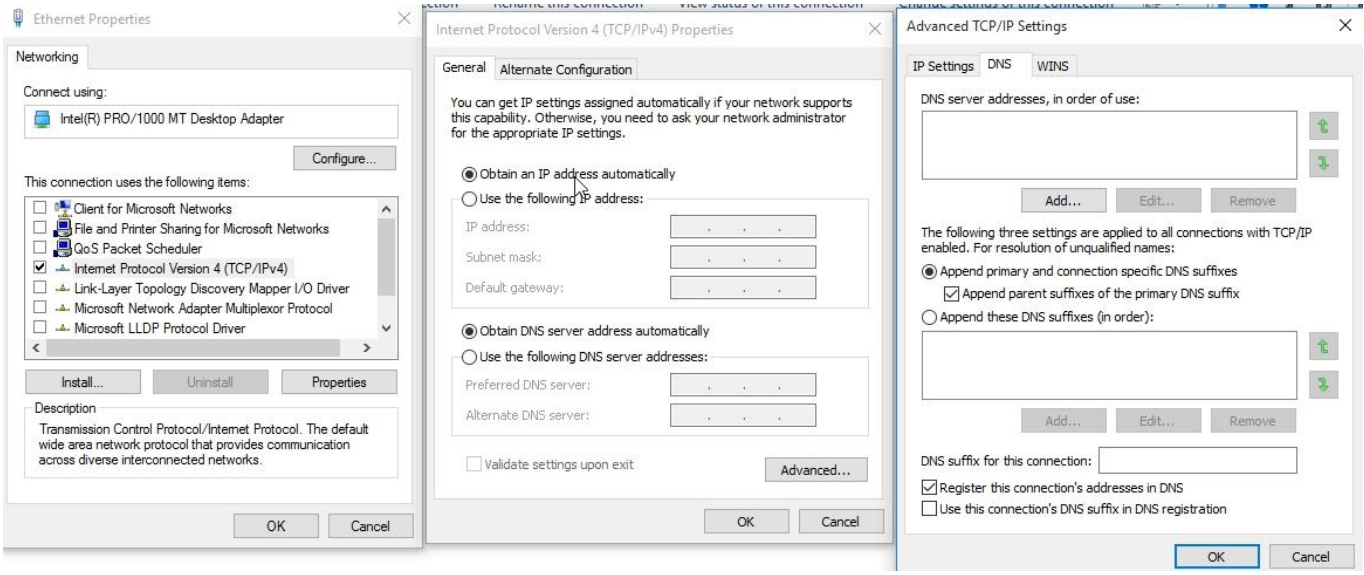
Δεξί κλικ στο Local Area Connection, επιλογή Properties\

Αποεπιλέγουμε τα ακόλουθα:

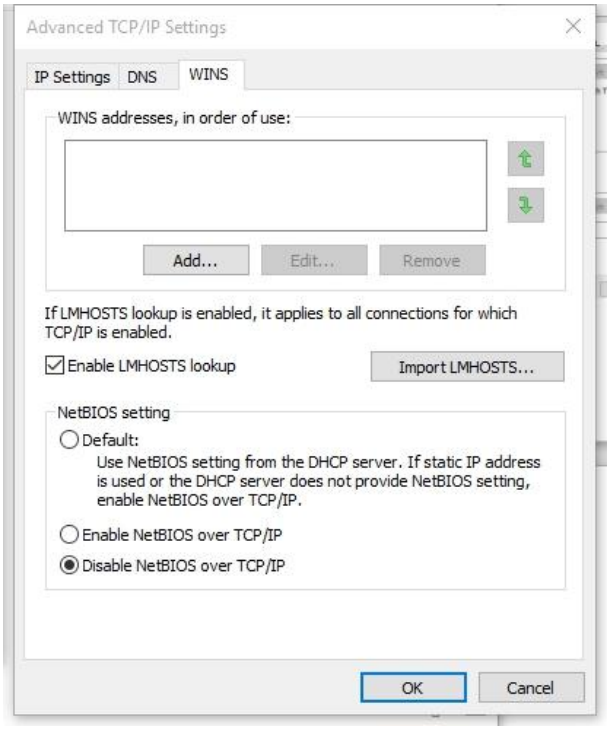
- Client for MS Networks
- File and Printer Sharing for Microsoft Networks
- QoS
- Microsoft Network Adapter Multiplexor Protocol
- Microsoft LLDP Protocol Driver
- LinkLayer Topology Discovery Mapper IO Driver
- Link Layer Topology Discovery Responder
- Internet protocol version 6



Επιλέγουμε 'Internet Protocol version 4 (TCP IPv4), επιλέγουμε Properties, επιλέγουμε Advanced, επιλέγουμε 'DNS' tab, αποεπιλέγουμε 'register this connections address in DNS'



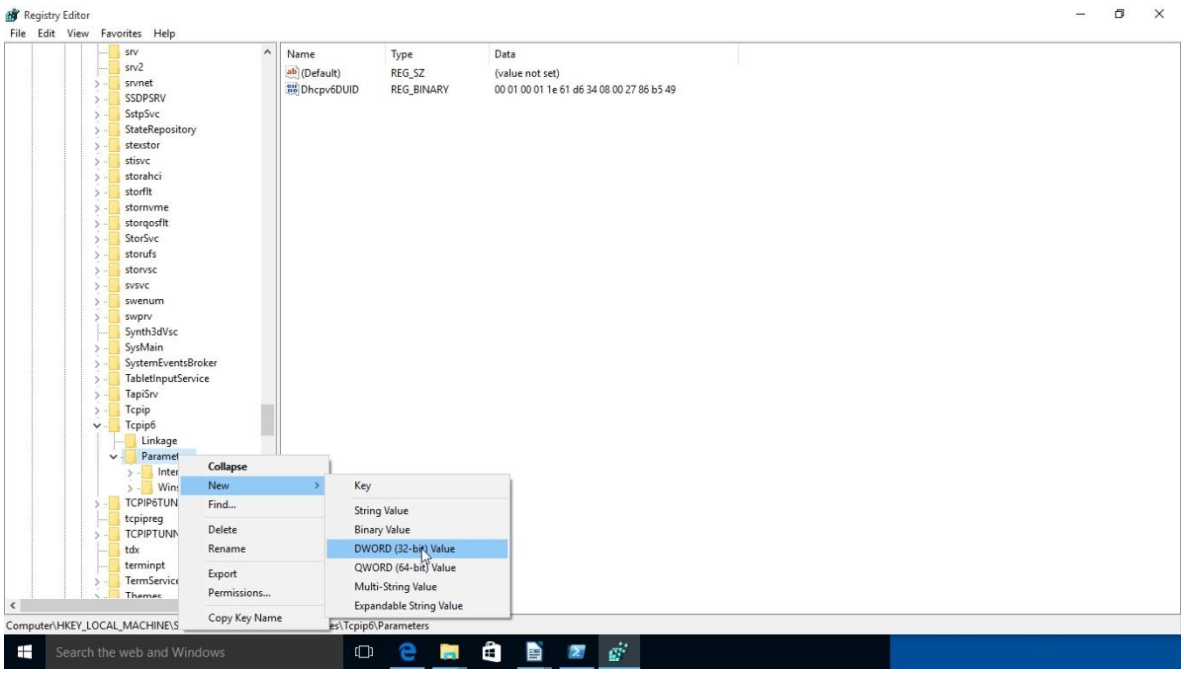
Επιλέγουμε 'WINS' tab, επιλέγουμε 'Disable NETBIOS over TCP/IP'



<u>Πλήρης Απενεργοποίηση του IPV6 (Disable IPV6 Totally)</u>

Εάν έχουμε έναν IPv6 router, παραλείπουμε τις παρακάτω οδηγίες.

./.



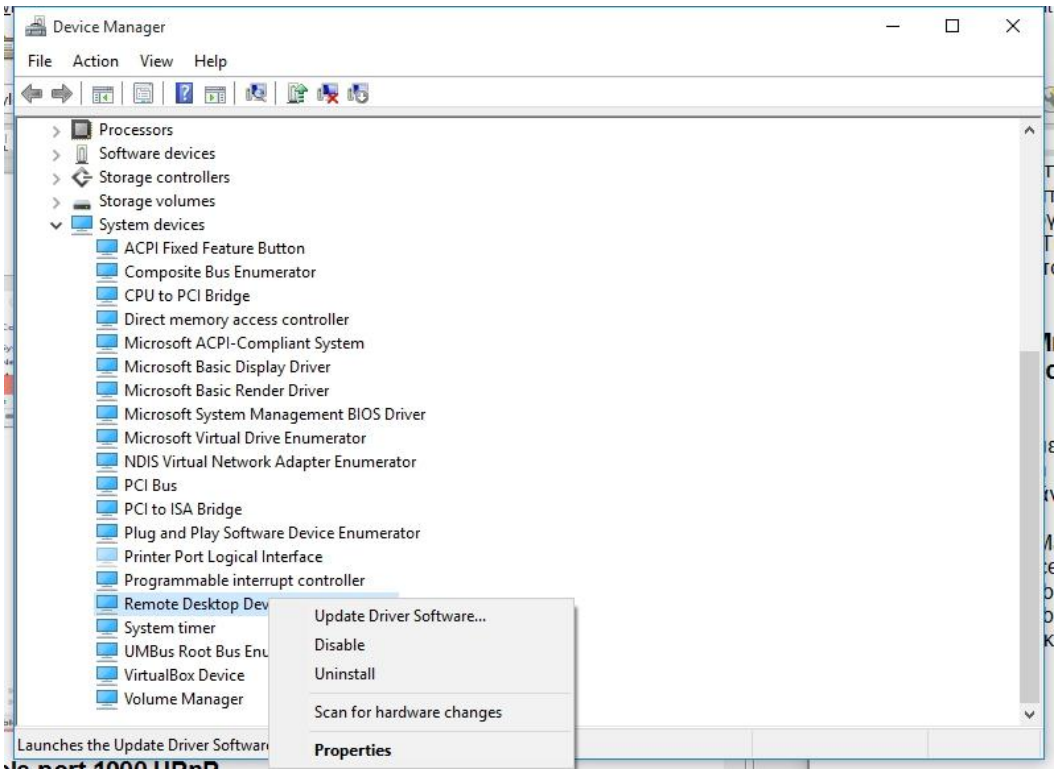
Στο search εκτελούμε την εντολή 'regedit', και στο κλειδι της registry “HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters”, κάνουμε δεξί κλικ και δημιουργούμε New entry of type DWORD(32bit) που το ονομάζουμε DisabledComponents.
Στη συνέχεια, κάνουμε διπλό κλικ, στην νέα εγγραφή DisabledComponents και εισάγουμε ένα από τα ακόλουθα :

FFFFFFFF για να απενεργοποιήσουμε όλα τα IPv6 components, εκτός από το IPv6 loopback interface, το οποίο δεν μπορεί να απενεργοποιηθεί.
0x01 για να απενεργοποιήσουμε όλα τα IPv6 tunnel interfaces. Αυτά περιλαμβάνουν το Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), το 6to4, και το Teredo. Εάν έχουμε ένα IPv6 router, τότε πρέπει να επιλέξουμε αυτή την περίπτωση.

Απενεργοποίηση Μη Χρησιμοποιούμενων Συσκευών tcpip6 (Disable unused tcpip6 Devices)

Όταν απενεργοποιούμε κάποια χαρακτηριστικά, απενεργοποιούμε και τα «εξαρτήματά» τους. Απενεργοποιήσαμε το IPv6, συνεπώς τώρα απενεργοποιούμε και τους παρακάτω οδηγούς (drivers0: Wan Miniport IPv6 driver, Teredo driver, ISATAP και IPv6 ARP driver. Αυτό μπορούμε να το κάνουμε ως εξής, πάμε στο:

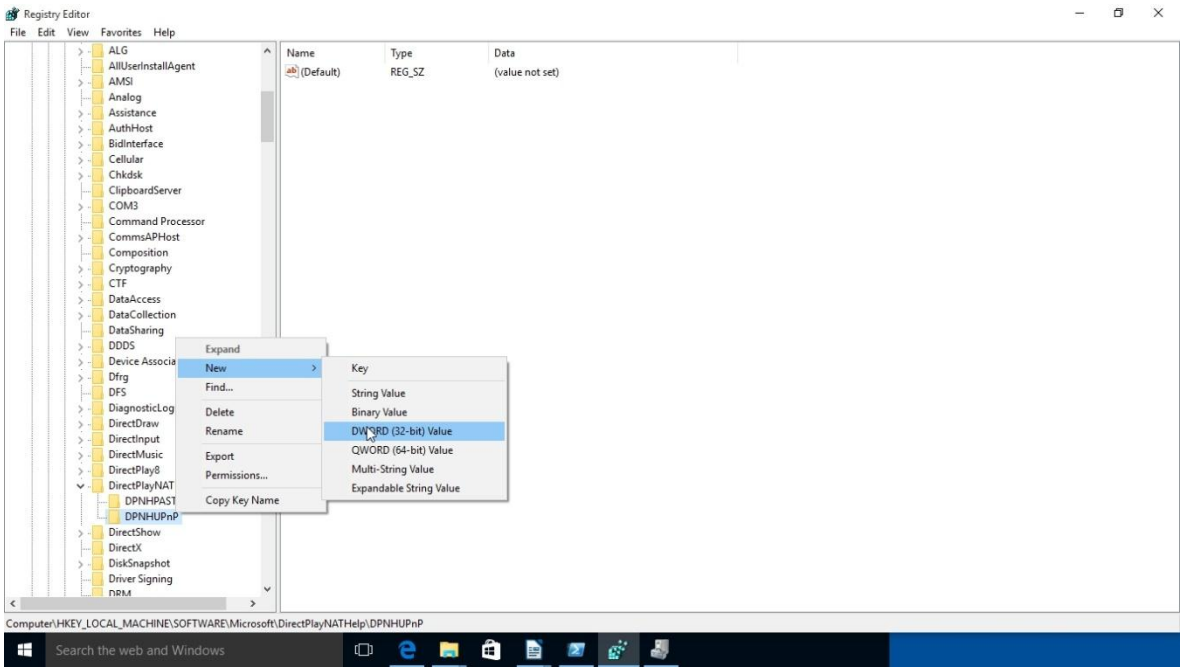
Control Panel > Device Manager, View menu > Show Hidden Devices
/System Devices\Remote Desktop Device Redirector Bus
/Network, disable Microsoft ISATAP adapter (Ipv6 tunnel)
/Network. disable Microsoft Kernel Debug Network Adapter
Στην συνέχεια κάνουμε επανεκκίνηση του υπολογιστή.



Απενεργοποίηση του UpnP (Disable port 1900 UPnP)

Το UPnP χρησιμοποιείται κυρίως σε παιχνίδια, όπου παραμετροποιεί το firewall, ώστε να επιτρέπει σε άλλους διαδικτυακούς παίχτες, να παίρνουν μέρος. Καλό θα ήταν να απενεργοποιηθεί. Εάν ο router ή το hardware firewall έχει την επιλογή απενεργοποίησης του UPnP, τότε απενεργοποιήστε το. Η απενεργοποίηση γίνεται μέσω registry, δίνουμε την εντολή:

c:\> regedit HKLM\Software\Microsoft\DirectplayNATHelp\DPNHUPnP
Δεξί κλικ (στο δεξί παράθυρο - right pane), νέα dword:32 bit, με όνομα UPnPMode Διπλό κλικ σ ’αυτό και θέτουμε την τιμή σε 2.



Απενεργοποίηση του SMB v1 Πρωτοκόλλου (Disable SMB v1 protocol)

Το πρωτόκολλο SMB είναι πρωτόκολλο διαμοιρασμού αρχείων και χρησιμοποιείται για τον διαμοιρασμό αρχείων και εκτυπωτών (File and Printer Sharing), καθώς και για επικοινωνία μεταξύ των διεργασιών (inter-process communication). Έχει τρεις (3) εκδόσεις. Η v2 και v3 δεν μπορούν να απενεργοποιηθούν. Υπάρχουν ιομορφικά λογισμικά (worms), τα οποία επιτίθενται στους διαμοιρασμούς SMB και αναλόγως το φορτίο, καταφέρνουν να αποκτήσουν πλήρη πρόσβαση του υπολογιστή.

Για να απενεργοποιήσουμε το SMB v1, ανοίγουμε ένα PowerShell prompt με δικαιώματα διαχειριστή (admin rights) και πληκτρολογούμε :

PS c:\> Set-SmbServerConfiguration -EnableSMB1Protocol $false

Για να ενεργοποιήσουμε πάλι το SMB v1, πληκτρολογούμε το εξής :

PS c:\> Set-SmbServerConfiguration -EnableSMB1Protocol $true

Απενεργοποίηση του IGMP (Internet Group Management Protocol)

Το συγκεκριμένο πρωτόκολλο δεν χρησιμοποιείτε καθόλου, συνεπώς το απενεργοποιούμε. Πάμε στο
search --> γράφουμε cmd.exe --> στο menu κάνουμε δεξι κλικ στο cmd.exe και επιλέγουμε "run as administrator" και δίνουμε την εντολή:
c:\> Netsh interface ipv4 set global mldlevel=none

Απενεργοποίηση Ανοιχτών Θυρών (Disabling Listening Ports)

Εάν εκτελέσουμε την εντολή '**netstat -abn**' στην γραμμή εντολών, θα εμφανιστούν ποιες πόρτες είναι ανοιχτές και είναι σε κατάσταση αναμονής (listening mode) στο δίκτυο. Θα πρέπει να αφήνουμε ανοιχτές μόνο τις πόρτες που χρειαζόμαστε, και τις υπόλοιπες να τις κλείνουμε.

Στα Windows 10 οι διεργασίες που ακούνε ('listening processes') και οι αντίστοιχοι αριθμοί πορτών τους είναι:

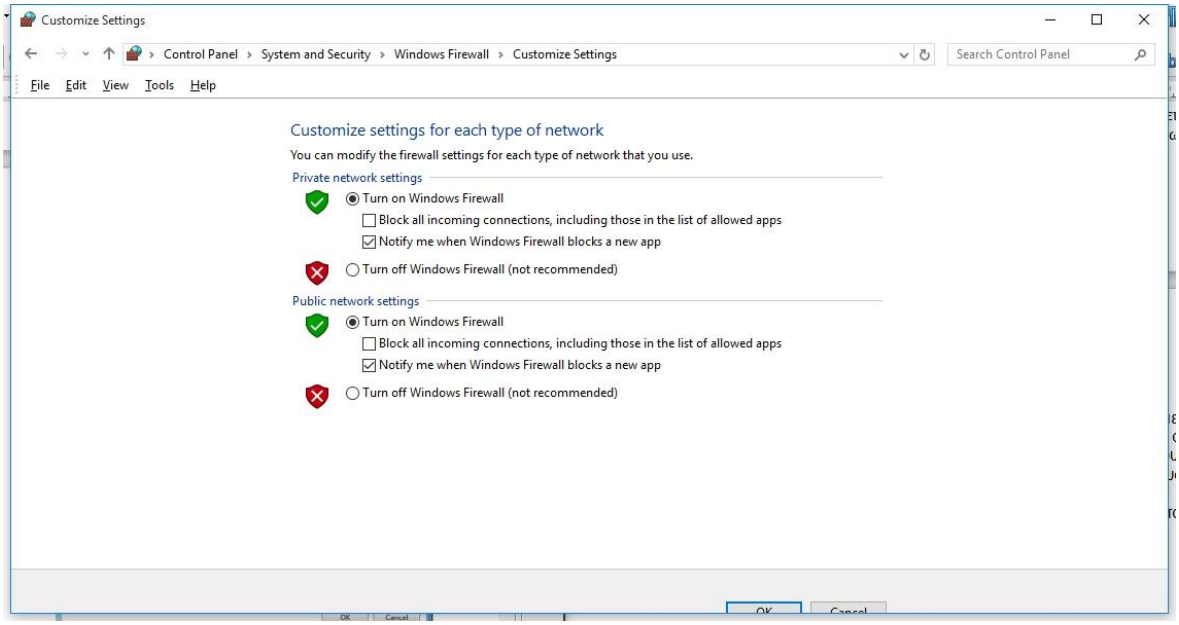
- RPCss (135)
- eventlog service (49409)
- Spoolsv (49410)
- schedule (49411)
- lsass.exe (49414)

Η προκαθορισμένη πολιτική του firewall για εισερχόμενη (inbound) κίνηση, είναι ρυθμισμένη σε 'block' για όλα τα network profiles (domain, private, public). Αυτό σημαίνει ότι κανένας "εξωτερικά" δεν μπορεί να πειράξει αυτές τις θύρες, εκτός εάν έχει γίνει κάποιος κανόνας εξαίρεσης ή το firewall είναι απενεργοποιημένο. Σε κάθε περίπτωση οι παραπάνω διεργασίες είναι απαραίτητες για τα Windows και δεν θα πρέπει να σταματήσουν. Συνεπώς μόνο οι παραπάνω διεργασίες θα είναι σε listening mode.

Προστασία από ανιχνεύσεις (scanning)

Για μεγαλύτερη ασφάλεια, πρέπει να χρησιμοποιούμε Firewall. Φροντίζουμε ώστε το Firewall των Windows να είναι ενεργοποιημένο. Η χρήση του είναι ιδιαίτερα σημαντική, ειδικά αν έχουμε laptop και συνδεόμαστε σε δίκτυα που δεν γνωρίζουμε. Έτσι, αποφεύγουμε τυχόν επιθέσεις από τρίτους που είναι συνδεδεμένοι στο ίδιο δίκτυο.

Για το ενσωματωμένο στα Windows Firewall, πάμε στο search , ή πατώντας το windows button, στη γραμμή αναζήτησης πληκτρολογούμε Windows Firewall και φροντίζουμε το firewall να είναι πάντα ενεργοποιημένο.



Εγκατάσταση επιπλέον τείχους ασφαλείας (Installing a 3rd Party Firewall)

Το firewall των Windows 10 είναι πολύ καλό, όμως αν επιθυμούμε, μπορούμε να εγκαταστήσουμε κάποιο άλλο firewall. Σημειώνουμε ότι εάν εγκαταστήσουμε κάποιο άλλο firewall, αυτόματα απενεργοποιείται το Windows 10 firewall, διότι εάν τρέχουν και τα 2 μαζί, θα δημιουργηθούν προβλήματα (conflicts).

Ένα πολύ καλό firewall, θεωρείται το **glasswire** firewall, το οποίο μας ενημερώνει και γραφικά για τις συνδέσεις, αλλά και μας ειδοποιεί για κάθε νέα σύνδεση.

ΤΜΗΜΑ 9
ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

Ασφάλεια του bios και screen saver

Παρότι δεν υπάρχει απόλυτος τρόπος προστασίας του υπολογιστή, οι παρακάτω συμβουλές σίγουρα θα δυσκολέψουν οποιονδήποτε αποκτήσει φυσική πρόσβαση σε αυτόν.

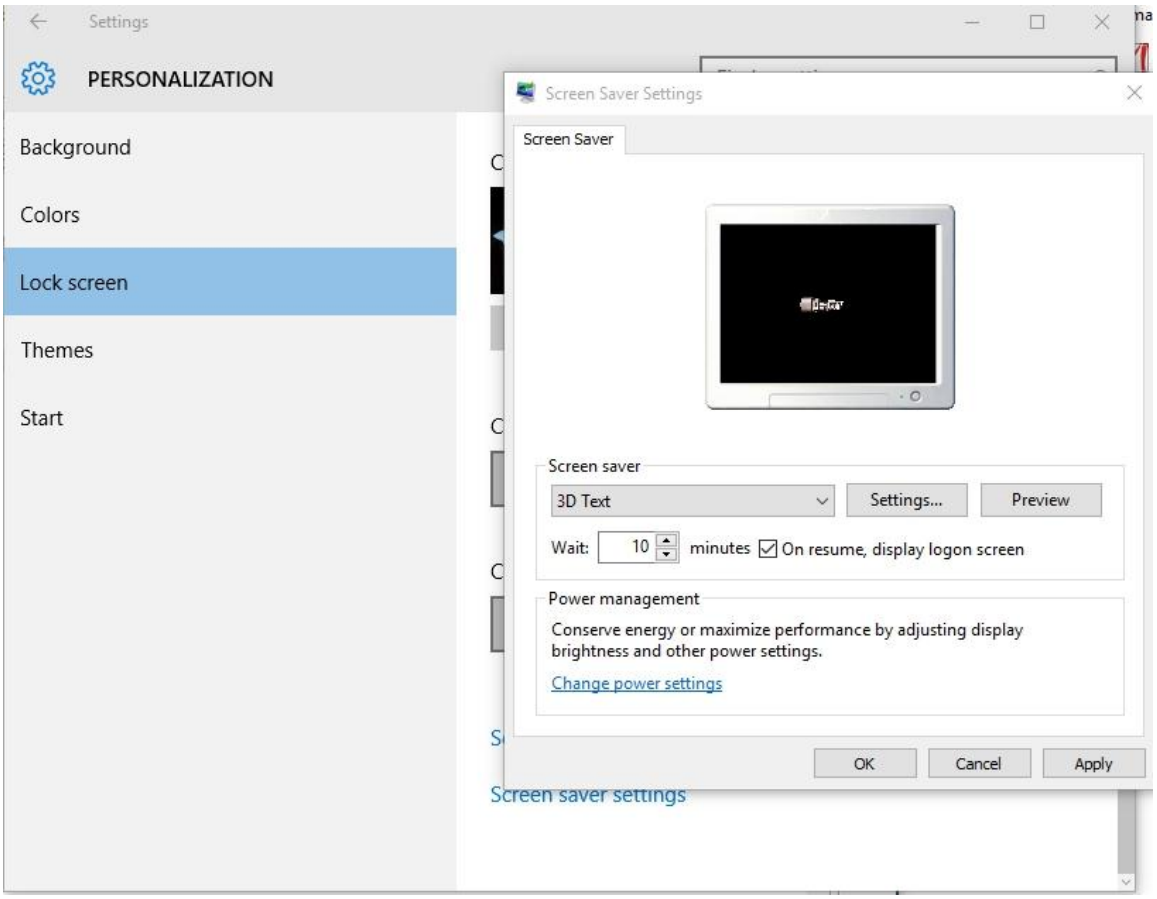
Πρώτα από όλα, προστατεύουμε το BIOS με συνθηματικό κωδικό και αφαιρούμε από το μενού εκκίνησης την επιλογή να γίνει boot με άλλο μέσο πλην του σκληρού μας δίσκου. Έτσι, δεν επιτρέπουμε σε κανέναν κακόβουλο χρήστη να μπει σε αυτό και να αλλάξει τις ρυθμίσεις του, για να εκκινήσει τον υπολογιστή μας, με τη χρήση CD, DVD ή USB, με άλλο λειτουργικό σύστημα και να υποκλέψει τα δεδομένα μας ή και να αλλάξει το συνθηματικό μας και να έχει στην συνέχεια πλήρη πρόσβαση στον υπολογιστή μας.

Επίσης, όταν απομακρυνόμαστε από τον χώρο εργασίας μας, ο υπολογιστής πρέπει να έχει συνθηματικό στο screen saver, για την προστασία από

κακόβουλους χρήστες.

Κάνουμε δεξί κλικ στην επιφάνεια εργασίας, επιλέγουμε Settings > Personalize > Lock Screen > Screen Saver settings. Το ρυθμίζουμε ώστε να περιμένει 10 λεπτά (minutes) και επιλέγουμε "On resume, display Logon screen".

Παράδειγμα :



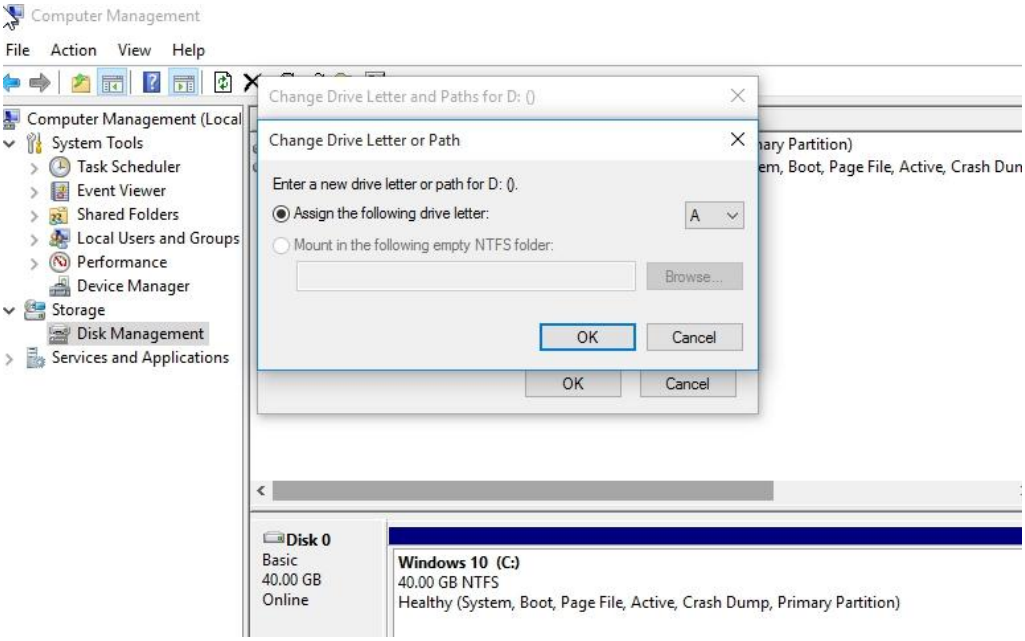
Syskey

Τα Windows έχουν ένα χαρακτηριστικό, το οποίο καλείται Syskey και μπορεί να αποθηκεύσει το κλειδί αποκρυπτογράφησης του συνθηματικού μας (password), σε ένα USB key. Τα συνθηματικά που χρησιμοποιούνται για να κάνουμε login, δεν αποθηκεύονται σε μορφή απλού κειμένου στα Windows, είναι κρυπτογραφημένα. Το κλειδί αποκρυπτογράφησης αυτών των συνθηματικών, μπορεί να αποθηκευτεί σε ένα drive A (Σημείωση: Πολλοί υπολογιστές δεν αναγνωρίζουν το drive A, διότι δεν χρησιμοποιείται πλέον). Αρχικά εισάγουμε το USB memory key, μετά κάνουμε δεξί κλικ στο Computer και επιλέγουμε Manage. Στη συνεχεία, Disk Management, κάνουμε δεξί κλικ στο USB memory stick, επιλέγουμε Change Drive Letter and Path. Κάνουμε κλικ Change button και το ονομάζουμε drive A.

Τώρα δίνουμε την εντολή "syskey". Κάνουμε κλικ στο Update button, επιλέγουμε

Store Startup Key on Floppy Disk. Εισάγουμε το USB memory key, και το κλειδί αποκρυπτογράφησης θα αποθηκευτεί στο USB.

Αφού γίνουν τα παραπάνω, όταν θα κάνουμε boot στα Windows, θα μας ζητάει να εισάγουμε ένα 'floppy disk', προκειμένου να συνεχίσει το boot.



Πλέον οποιοσδήποτε προσπαθεί να εκκινήσει τον υπολογιστή, θα χρειάζεται το USB memory stick, όπως και το συνθηματικό χρήστη.

./.

ΤΜΗΜΑ 10
ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ

Antivirus

Η χρήση λογισμικού antivirus και anti-spyware είναι επιβεβλημένη λόγω της πληθώρας των κακόβουλων προγραμμάτων που κυκλοφορούν στο διαδίκτυο. Τα Windows 10 έχουν το Windows Defender antivirus. Εκτός από τα εμπορικά προγράμματα (που απαιτούν αγορά του προϊόντος), μπορούμε να χρησιμοποιήσουμε και δωρεάν λογισμικά, όπως:

AVG (http://www.avg.com/us-en/free-antivirus-download)
AVAST (http://www.avast.com/free-antivirus-download)
http://www.pcmag.com/article2/0,2817,2388652,00.asp

Ένας απλός τρόπος για να ελέγξουμε εάν έχουμε κάποιο antivirus ενεργό, είναι να κάνουμε τα ακόλουθα 2 πράγματα :

1. Ελέγχουμε ότι το antivirus είναι ενεργοποιημένο. Πάμε στο http://www.eicar.org/86-0-Intended-use.html και αντιγράφουμε την γραμμή κάτω από την ετικέτα «test virus line of text», σε ένα notepad, το σώζουμε και προσπαθούμε να το ανοίξουμε ξανά. Το antivirus θα πρέπει να το ανιχνεύσει.
2. Πραγματοποιούμε ένα antivirus scan.

Επίσης, χρειάζεται να δημιουργηθεί ένας εξερχόμενος (outbound) κανόνας στο firewall, ο οποίος θα επιτρέπει στο antivirus να βρίσκει / κατεβάζει τις ενημερώσεις των υπογραφών ιομορφικού λογισμικού (signature updates).

On-line έλεγχος για ιομορφικό λογισμικό

Στην περίπτωση που έχουμε μία άγνωστη εφαρμογή ή URL ή αρχείο (.doc, .xls, .pdf) και έχουμε αμφιβολίες για το αν έχει ή όχι ιομορφικό κώδικα, τότε μπορούμε να το “ανεβάσουμε” (upload) σε on-line υπηρεσίες που το ελέγχουν με μία σειρά αντι-ιϊκών και να μας δοθεί μία αναφορά αν είναι ύποπτο ή όχι.

Σχετικοί σύνδεσμοι:
http://www.virustotal.com
http://virusscan.jotti.org/en
http://www.virscan.org/

Στην περίπτωση που έχουμε εντοπίσει ένα εκτελέσιμο αρχείο (.exe), το οποίο δεν το αναγνωρίζουμε, μπορούμε εκτός από την παραπάνω διαδικασία, να το ανεβάσουμε σε online sandboxes, τα οποία πραγματοποιούν ανάλυση συμπεριφοράς, για το τι ακριβώς αυτό κάνει.

Σχετικοί σύνδεσμοι:
https://malwr.com/
http://anubis.iseclab.org/
http://www.threatexpert.com/submit.aspx
http://www.threattrack.com/
http://wepawet.iseclab.org/

Keyloggers και Screen Grabbers

Στα ιομορφικά λογισμικά, ανήκουν και τα λογισμικά τύπου keyloggers και Screen Grabbers. Σκοπός τους είναι να αποτυπώσουν, τι έγραψε και τι είδε ο χρήστης εν αγνοία του, για να του αποσπάσουν κωδικούς για διάφορες υπηρεσίες, όπως πιστωτικές κάρτες, e-banking, κ.α. Τα προγράμματα antivirus δεν τα εντοπίζουν. Δύο προγράμματα προστασίας, αποκλειστικά για τέτοιου είδους κακόβουλο λογισμικό είναι τα:
Zemana AntiLogger (http://www.zemana.com) και το
KeyScrambler (http://www,qfxsoftware.com) [Μόνο για αντι-keylogger]

ΤΜΗΜΑ 11
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΛΟΓΙΣΜΙΚΟΥ (SOFTWARE RESTRICTION POLICY)

Ενεργοποίηση του Software Restriction Policy

Η ενεργοποίηση της Πολιτικής Ασφαλείας Λογισμικού (Software Restriction Policy), αποτρέπει προγράμματα να εκτελεστούν στον υπολογιστή μας, εκτός εάν αυτά βρίσκονται στους φακέλους **\Program Files** ή **\Windows**. Αυτό σημαίνει ότι κάθε ιομορφικό λογισμικό, το οποίο μεταφορτώνεται (download) σε φακέλους διαφορετικούς από τους παραπάνω, δεν θα εκτελεστεί.

Ρύθμιση του AppLocker

Η εφαρμογή AppLocker (είναι εγκατεστημένη στην έκδοση enterprise) λειτουργεί όπως και το Software Restriction Policy (SRP), αλλά είναι πιο ευέλικτη. Την ενεργοποιούμε για να έχουμε καλύτερη ασφάλεια στον υπολογιστή μας. Μπορούμε να ρυθμίσουμε ποιος επιτρέπεται να εκτελέσει οποιοδήποτε πρόγραμμα ή script.

Μπορούμε να εφαρμόσουμε κανόνες στα παρακάτω:

- Εκτελέσιμα : exe and com
- Scripts : js, ps1, vbs, cmd and bat
- Αρχεία Windows Installer : msi and msp
- Dynamic-link libraries : dll and ocx (Αυτή η δυνατότητα πρέπει να ενεργοποιηθεί, δεν είναι εξ ορισμού ενεργοποιημένη)

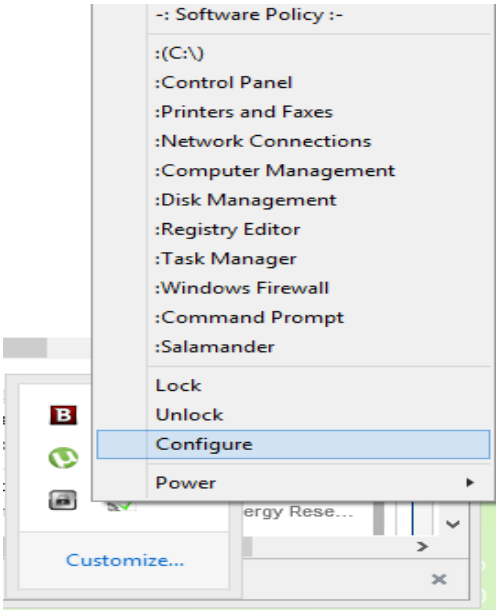
- Packaged app Rules : aappx (Windows 8 & 10 only)

Η γενική ιδέα είναι να έχουμε τον έλεγχο σε ποια προγράμματα μπορούν να εκτελεστούν στον υπολογιστή μας και ποιος έχει το δικαίωμα να το εκτελέσει.

Λογισμικό Simple Software Restriction Policy

Πρόκειται για μία πιο ευέλικτη εφαρμογή (δωρεάν), που αντικαθιστά την εφαρμογή Applocker. Είναι πολύ εύκολη στην παραμετροποίησή του. Το πρόγραμμα εγκαθίσταται στην διαδρομή \Windows\SoftwarePolicy. Η παραμετροποίηση πραγματοποιείται μέσω ενός .ini file, το οποίο είναι προσβάσιμο και παραμετροποιήσιμο από το μενού του. Υπάρχουν κάποιες από τις εξ ορισμού ρυθμίσεις που χρειάζονται αλλαγές. Τις αλλαγές αυτές μπορούμε να τις κάνουμε ακολουθώντας τα παρακάτω βήματα.

Κάνουμε δεξί κλικ στο program's systray icon και επιλέγουμε Configure.



θα ξεκινήσει αυτόματα το Notepad, παρουσιάζοντας τις εξ ορισμού ρυθμίσεις. Επεξεργαζόμαστε τα παρακάτω και αλλάζουμε την τιμή από 0 σε 2, όπως παρακάτω :

AdminMenuPasswordLevel=2

Στη συνέχεια προσθέτουμε από κάτω τις παρακάτω γραμμές:

[Disallowed]
c:\windows\debug\WIA=1
c:\windows\Registration\CRMLog=1
c:\windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}=1
c:\windows\System32\com\dmp=1

c:\windows\System32\FxsTmp=1
c:\windows\System32\spool\PRINTERS=1
c:\windows\System32\spool\drivers\color=1
c:\windows\System32\Tasks=1
c:\windows\SysWOW64\com\dmp=1
c:\windows\SysWOW64\FxsTmp=1
c:\windows\SysWOW64\Tasks=1
c:\windows\Tasks=1
c:\windows\Temp=1
c:\windows\tracing=1

Τα παραπάνω παραμετροποιούν το πρόγραμμα, ώστε αυτό να ζητάει ένα συνθηματικό διαχειριστή των Windows. Επίσης ασφαλίζει τα αναφερόμενα μονοπάτια (paths) κάτω από τον φάκελο \Windows, τα οποία μπορούν να αλλαχθούν από τους χρήστες, ώστε να μην μπορεί να εκτελεστεί ιομορφικό λογισμικό (malware) από εκεί.

Επίσης, μπορούμε να προσθέσουμε ένα “;” μπροστά από αυτές τις γραμμές, ώστε να αφαιρεθούν επιπλέον στοιχεία του Μενού:

;(C:\)=explorer.exe C:\
;Control Panel=control.exe
;Printers and Faxes=control printers
;Network Connections=ncpa.cpl
;Computer Management=compmgmt.msc
;Disk Management=diskmgmt.msc
;Registry Editor=regedit.exe
;Task Manager=taskmgr.exe
;Windows Firewall=firewall.cpl
;Command Prompt=cmd.exe
;Salamander=salamand.exe

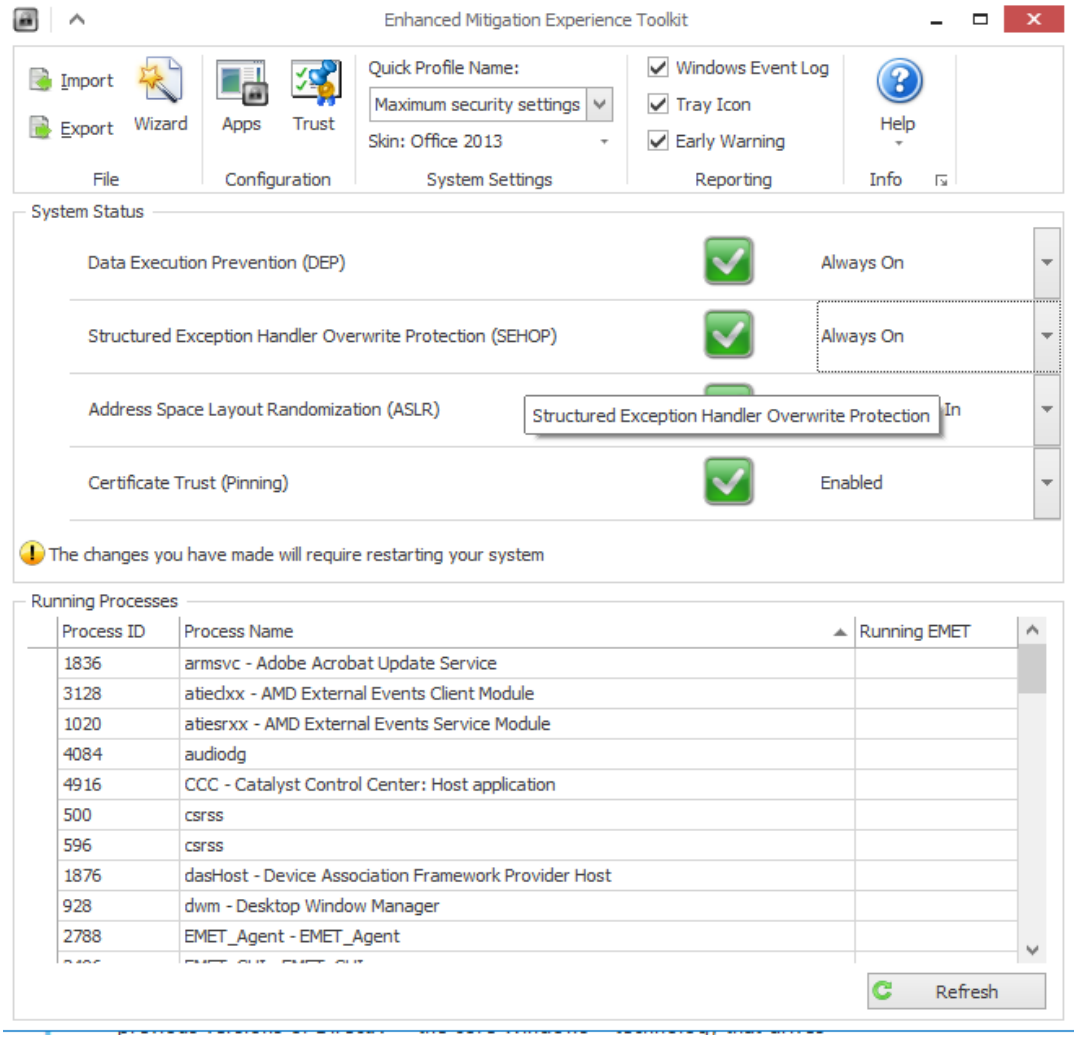
Εγκατάσταση του EMET (Enhanced Mitigation Experience Toolkit)

https://www.microsoft.com/en-us/download/details.aspx?id=50766

Η εγκατάσταση του EMET, είναι σημαντική και απαραίτητη. Αυτό που μας παρέχει είναι μία επιπλέον ασφάλεια σε επίπεδο εφαρμογής, ώστε ακόμα και αν υπάρχει ένα exploit (εκμετάλλευση αδυναμίας) για την συγκεκριμένη εφαρμογή, το EMET εμποδίζει την επιτυχή εκμετάλλευση.

Για την εγκατάσταση του EMET ακολουθούμε τον οδηγό. Για την παραμετροποίησή του εκτελούμε το και επιλέγουμε ‘Configure System button,’, και ρυθμίζουμε τα ακόλουθα :
DEP --> always on.
SEHOP --> always on
ASLR --> application opt in.

defaults:
DEP : application Opt In
SEHOP : application Opt In
ASLR: application Opt In
Pinning: Enabled



Επιλέγουμε το "Apps" button, και μετά το "Add Application" και αναζητούμε για να προσθέσουμε τα ακόλουθα:

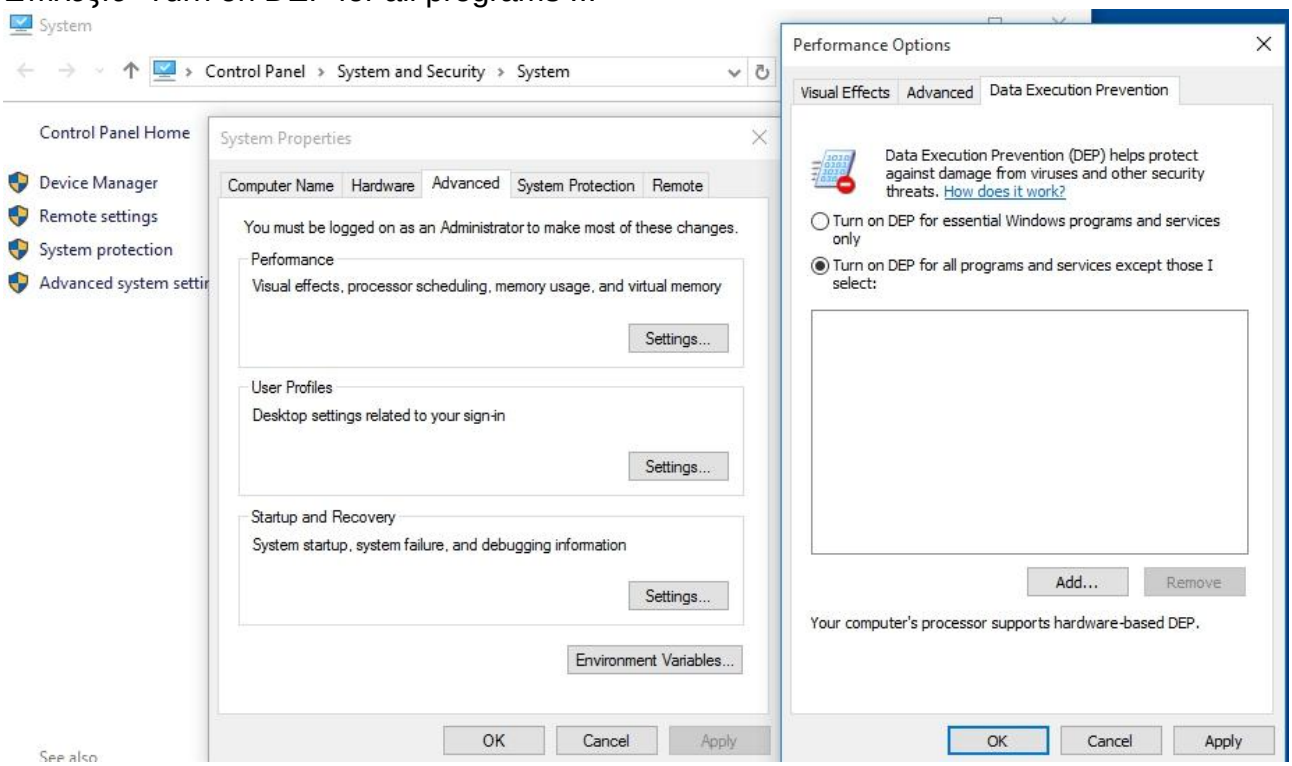
\Windows\System32\wuauclt.exe
\Windows\servicing\trustedinstaller.exe
Το antivirus λογισμικό, εάν διαθέτουμε.

Προσθέτουμε επίσης όλους τους browsers, τα προγράμματα συζήτησης (chat clients) και άλλα προγράμματα που συνδέονται στο διαδίκτυο (internet). Αυτό περιλαμβάνει όλα τα προγράμματα, που παίρνουν δεδομένα (input) από λογισμικό που έχουμε μεταφορτώσει (download), όπως media players, Adobe Reader.

Ενεργοποίηση αποτροπής εκτέλεσης δεδομένων - Enable DEP (Data Execution Prevention)

Το DEP είναι μια τεχνολογία, η οποία ματαιώνει κάποιους τύπους επιθέσεων, όταν είναι κωδικοποιημένες με συγκεκριμένο τρόπο. Το χαρακτηριστικό είναι ενεργοποιημένο από προεπιλογή, αλλά προστατεύει μόνο τα εκτελέσιμα των Windows.
Εάν έχουμε εγκατεστημένο το EMET, αυτό το χαρακτηριστικό απενεργοποιείται, γιατί το EMET αναλαμβάνει τη διαχείριση του DEP.

Δεξί κλικ **My PC >** Properties > Advanced System Settings
> Performance Settings button > Data Execution Prevention Tab
Επιλέξτε "Turn on DEP for all programs ..."



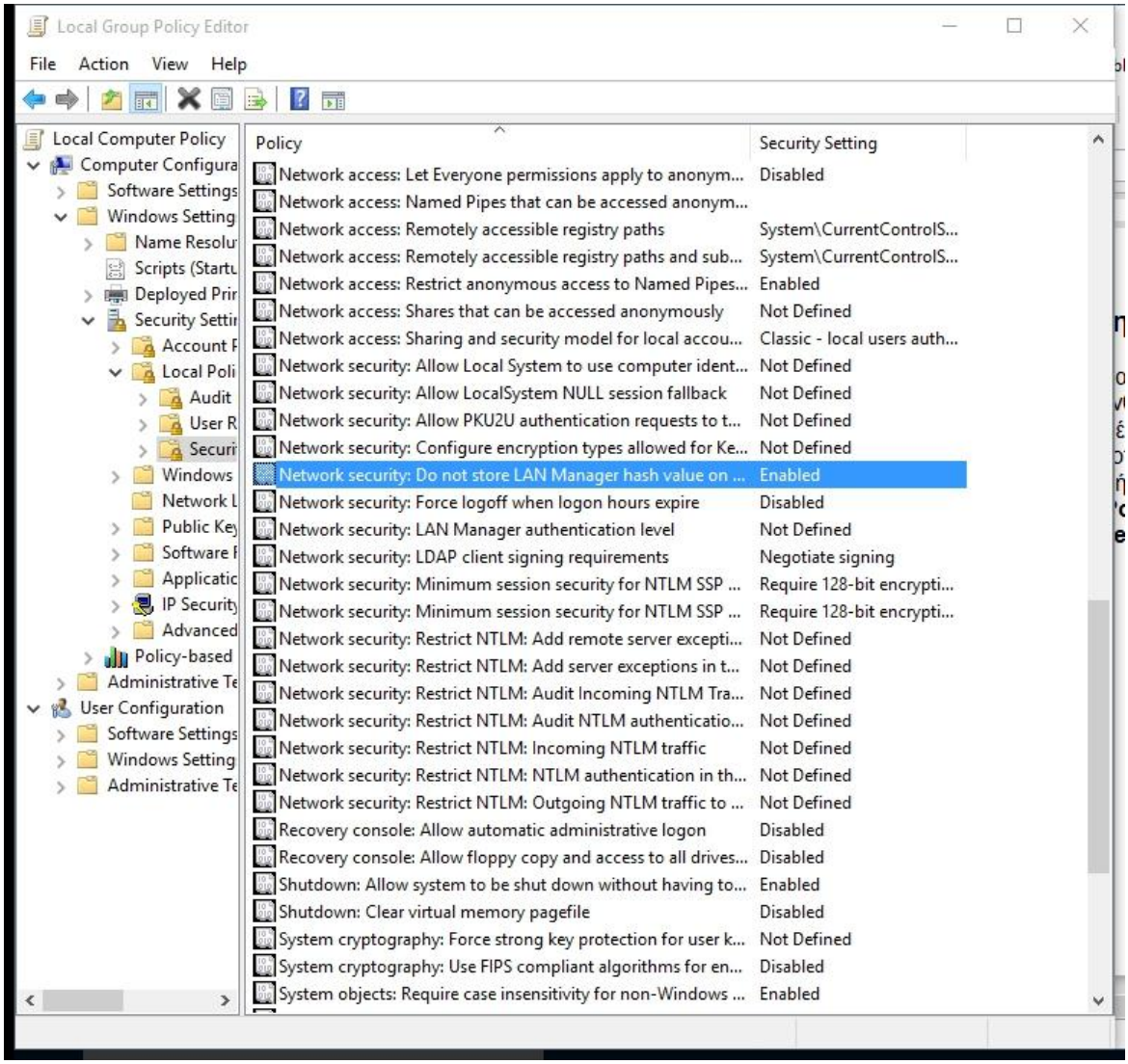
Προστασία συνθηματικών στο διαδίκτυο

Δεν πρέπει να επιτρέπουμε στον browser να θυμάται τα συνθηματικά πρόσβασης σε σελίδες. Αν κάποιος κακόβουλος χρήστης αποκτήσει πρόσβαση στον υπολογιστή μας, τότε πολύ εύκολα μπορεί να ανακτήσει τα συνθηματικά που έχει αποθηκεύσει ο browser.

Προστασία τοπικών συνθηματικών χρήστη

Στην περίπτωση που κάποιος κακόβουλος χρήστης αποκτήσει το κρυπτογραφημένο από το λειτουργικό σύστημα συνθηματικό κάποιου χρήστη, μπορεί εύκολα να το αποκρυπτογραφήσει εάν αυτό έχει κρυπτογραφηθεί με το

LMHASH. Η διαδικασία που ακολουθούμε για να το απενεργοποιήσουμε είναι η παρακάτω: στο search , ή πατώντας το windows button (□), στη γραμμή αναζήτησης πληκτρολογούμε **gpedit.msc** και πατάμε **enter**. Στο **Local Computer Policy**, πηγαίνουμε στη θέση **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, **Security Options** όπως φαίνεται και στην παρακάτω εικόνα :



Στη λίστα με τις διαθέσιμες πολιτικές (policies), κάνουμε διπλό κλικ στο **Network security: Do not store LAN Manager hash value on next password change**. Στο παράθυρο που εμφανίζεται επιλέγουμε **Enabled** και στην συνέχεια **OK**.

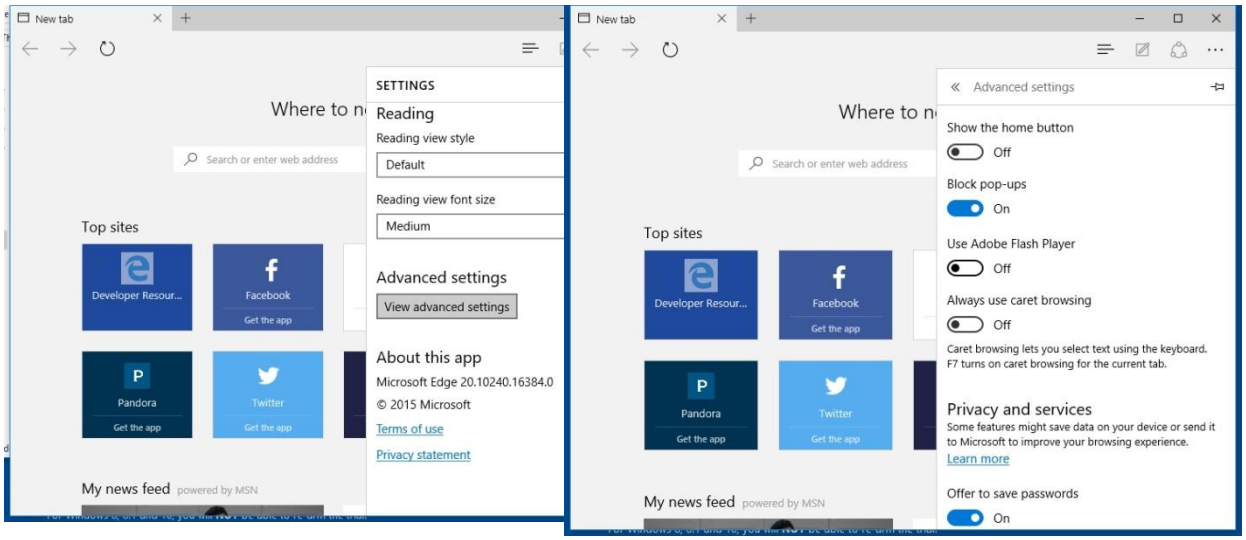
ΤΜΗΜΑ 12
ΑΣΦΆΛΕΙΑ ΕΦΑΡΜΟΓΏΝ

Ασφάλεια Φυλλομετρητών (Browsers)

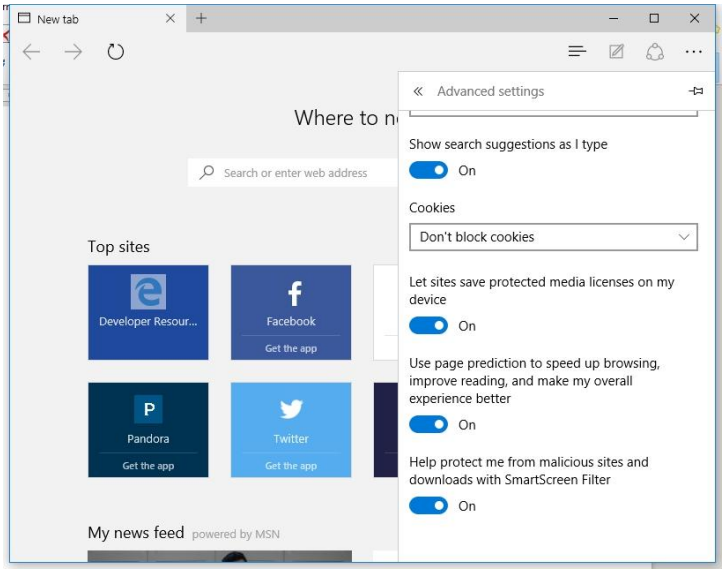
Ο **Edge** είναι το προεπιλεγμένο πρόγραμμα περιήγησης στο Web των Windows 10, και έχει μερικά νέα χαρακτηριστικά ασφαλείας, όπως η αφαίρεση υποστήριξης ActiveX, VBScript, Browser Helper Objects (BHO) και VML. Είναι επίσης μια εφαρμογή των Windows, σε περιβάλλον sandbox. Έχει επίσης έξυπνο φίλτρο οθόνης, όπως ο IE. Υποστηρίζει το W3C πρότυπο «Πολιτική Ασφάλειας Περιεχομένου», και έχει επίσης HTTP Strict Ασφάλειας Μεταφορών. Είναι, επίσης, ένα πρόγραμμα περιήγησης 64 bit, και χρησιμοποιεί ASLR (Address Space Layout Randomization) πλήρως. Υπάρχει επίσης ένα νέο χαρακτηριστικό το οποίο ονομάζεται «Control Flow Guard», για να ελέγχει τις επιθέσεις στην μνήμη.

Καλή πρακτική ασφαλείας:

Ανοίγουμε τον Edge, κάνουμε κλικ στο Ρυθμίσεις (το κουμπί "...". Κάνουμε κλικ στο settings και στη συνέχεια,«View advanced settings».
Γυρίζουμε σε off το «Use Adobe Flash». Πολλά sites χρησιμοποιούν πλέον HTML 5 και έτσι δεν χρειάζεται πλέον το Flash για να προβάλλουμε τα videos. Το Flash είχε πολλά τρωτά σημεία ασφάλειας.



Ρυθμίζουμε σε **on** το «Help protect me from malicious sites and downloads with SmartScreen Filter» Επειδή τα προγράμματα περιήγησης είναι η κύρια διασύνδεση με το διαδίκτυο, και χρησιμοποιείται από όλους, είναι ένα πρωταρχικός φορέας επίθεσης. Οι επιτιθέμενοι έχουν την δυνατότητα να τροποποιήσουν μια ιστοσελίδα για να στέλνει / κατεβάζει ιομορφικό λογισμικό, χρησιμοποιώντας τυχόν αδυναμίες ασφαλείας στο πρόγραμμα περιήγησης ή στα προγράμματα που καλεί αυτό.



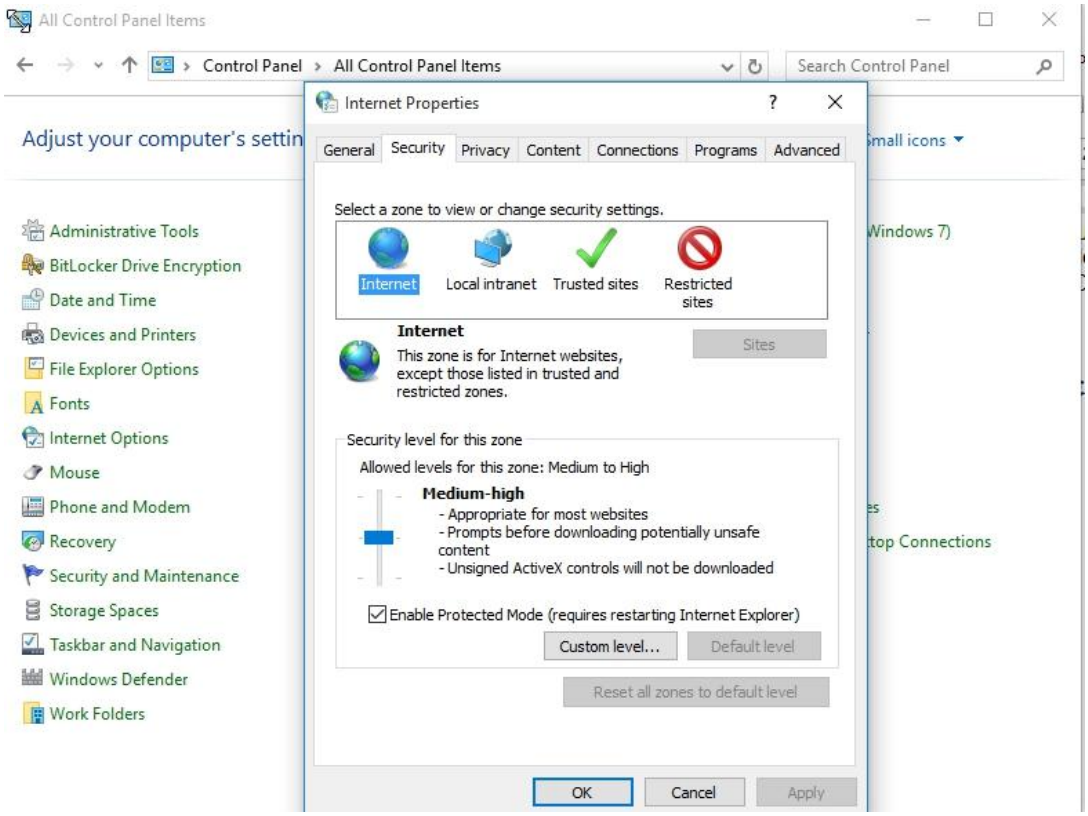
Ρύθμιση του IE ώστε να χρησιμοποιεί Protected Mode

Ο **Internet Explorer** είναι ο πιο γνωστός φυλλομετρητής διότι είναι εγκατεστημένος από προεπιλογή. Οι φυλλομετρητές αποτελούν κύριο στόχο επιθέσεων μέσω διαδικτύου. Οι επιτιθέμενοι επιτίθενται σε μια ιστοσελίδα, διαμορφώνοντας την έτσι, ώστε να διακινεί κακόβουλο λογισμικό (malware), εκμεταλλευόμενοι τα κενά ασφαλείας του φυλλομετρητή. Ο Internet Explorer έχει ένα πολύ σημαντικό μηχανισμό άμυνας, ο οποίος καλείται Protected Mode. Πρόκειται για μια άλλη ονομασία των Integrity Levels. Βασικά, ολόκληρο το σύστημα θεωρείται ως Medium integrity. Όμως, προγράμματα που δέχονται συχνά επιθέσεις, όπως ο Internet Explorer, θεωρούνται ως Low integrity. Τα Low integrity προγράμματα, δεν είναι δυνατό να παραμετροποιηθούν, ώστε να αλλάξουν σε Medium. Συνεπώς, εάν κάποιος παραβιάσει τον IE και αποκτήσει πρόσβαση στον υπολογιστή μας, δεν μπορεί να παραμετροποιήσει (να αλλάξει) το σύστημα. Μπορούμε να ρυθμίσουμε το integrity level ενός προγράμματος, έτσι ώστε να ρυθμίσουμε τους άλλους φυλλομετρητές να χρησιμοποιούν την λειτουργεία Protected Mode.

Γνωστές εναλλακτικές του IE είναι οι Firefox, Opera και Chrome. Έχουν βρεθεί πολλά κενά ασφαλείας και σε αυτούς, όπως και στον IE, αλλά φημολογούνται ως πιο ασφαλή, κυρίως διότι δεν χρησιμοποιούν την εφαρμογή ActiveX.

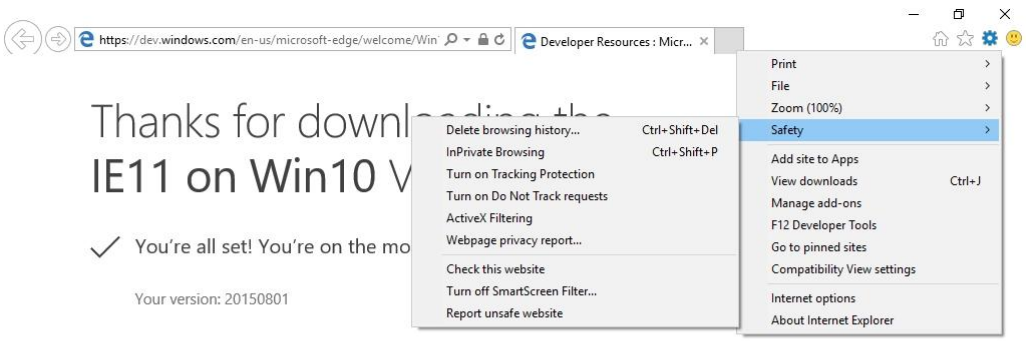
Για να ρυθμίσουμε τον IE να χρησιμοποιείται σε protected mode, ενεργούμε ως εξής, πάμε στο:

Control Panel > Internet Options > Security Tab
Επιλογή του Protected Mode for all zones



Ρύθμιση του IE ώστε να χρησιμοποιεί φίλτρο στο ActiveX

Ανοίγουμε τον IE, Internet Explorer, Gear icon > Safety / > επιλέγουμε ActiveX Filtering

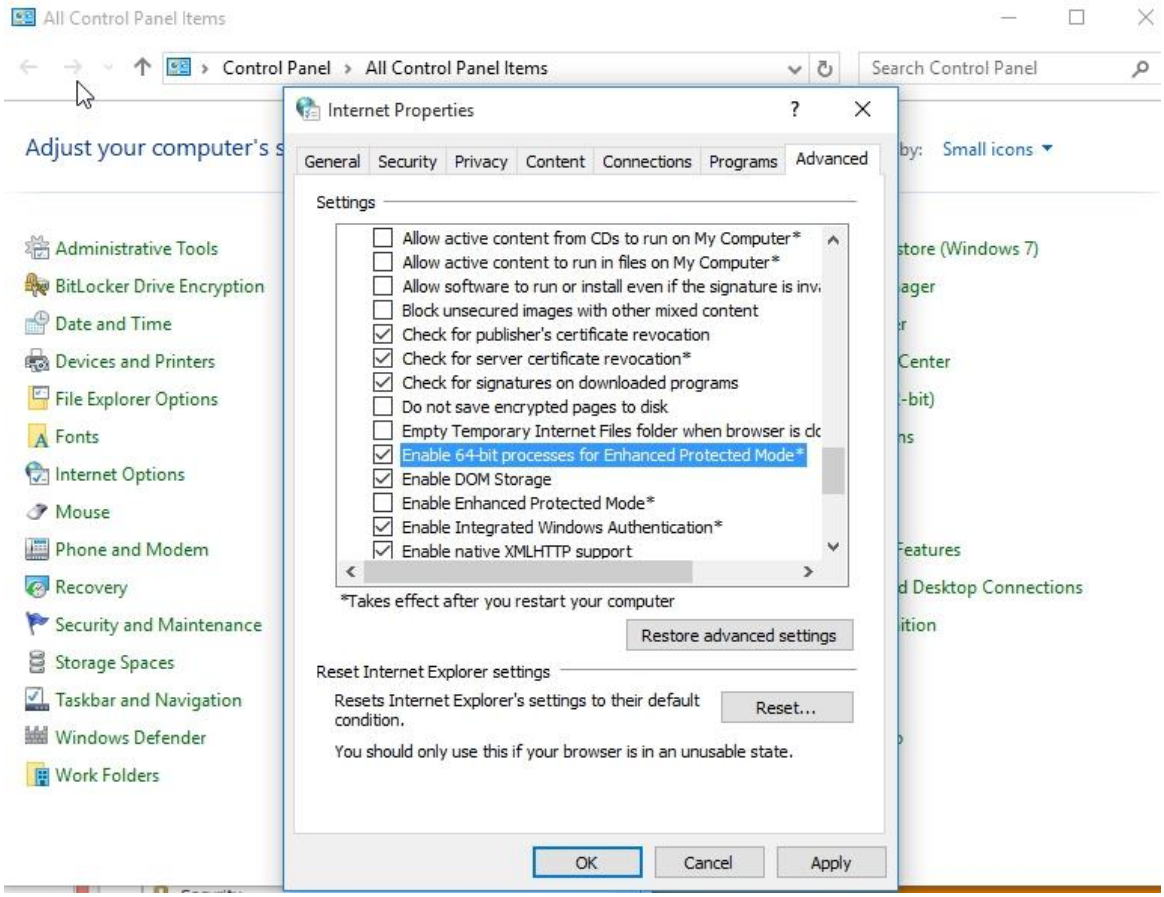


./.

Ρύθμιση του IE ώστε να χρησιμοποιεί το Enhanced Protected Mode

Στα Windows υπάρχει η ρύθμιση Enhanced Protected Mode, η οποία προστατεύει προσωπικά αρχεία και φακέλους, όπως ο φάκελος έγγραφα. Για να ρυθμίσουμε τον IE ώστε να χρησιμοποιεί το Enhanced Protected Mode, πάμε στο:

Control Panel > Internet Options > Advanced και εδώ στο Security section επιλέγουμε "Enable 64 bit Processes for Enhanced Protected Mode"



Ρύθμιση του Mozilla Firefox

Ο Mozilla Firefox είναι ένα λογισμικό ανοιχτού κώδικα και μπορεί να ασφαλιστεί καλύτερα εάν εγκαταστήσουμε ορισμένα plug-ins. Το πιο δημοφιλές είναι το **No-Script**, το οποίο μπλοκάρει την εκτέλεση JavaScript, εάν κάποια ιστοσελίδα δεν θεωρείται αξιόπιστη. Επιπρόσθετα, το **AdBlock Plus** χρησιμοποιείται προκειμένου να μπλοκάρει κακόβουλες διαφημίσεις, αφαιρώντας αυτές από την ιστοσελίδα. Ένα άλλο γνωστό plug-in που χρησιμοποιείται είναι το **WOT** (web of trust). Αυτό το plug-in μας κρατά ενήμερους, όταν κάποια ιστοσελίδα διακινεί κακόβουλο λογισμικό. Τέλος υπάρχει ένα ακόμα plug-in, το οποίο διατίθεται από το Mcafee, και ονομάζεται **SiteAdvisor**.

Ρύθμιση σε Low Integrity του Firefox

Μπορούμε να αυξήσουμε το επίπεδο ασφαλείας του υπολογιστή μας, ρυθμίζοντας τον Firefox σε low integrity. Ανοίγουμε μία γραμμή εντολών (command prompt) με αυξημένα δικαιώματα (run us administrator), και εκτελούμε τις ακόλουθες εντολές, με τη σειρά, μια προς μια, αντικαθιστώντας τον λογαριασμό χρήστη (account name), με τον αντίστοιχο δικό μας:

```
icacls "C:\Program Files (x86)\Mozilla Firefox\Firefox.exe" /setintegritylevel low
icacls "C:\Users\<yourAccName>\AppData\Local\Temp" /setintegritylevel(oi)(ci)
low /t
icacls "C:\Users\<yourAccName>\AppData\Local\Mozilla" /setintegritylevel(oi)(ci)
low /t
icacls "C:\Users\<yourAccName>\AppData\Roaming\Mozilla"
/setintegritylevel(oi)(ci) low /t
icacls "C:\Users\<yourAccName>\Downloads" /setintegritylevel(oi)(ci) low /t
icacls "C:\Users\<nextAccName>\AppData\Local\Temp" /setintegritylevel(oi)(ci)
low /t
icacls "C:\Users\<nextAccName>\AppData\Local\Mozilla" /setintegritylevel(oi)(ci)
low /t
icacls "C:\Users\<nextAccName>\AppData\Roaming\Mozilla"
/setintegritylevel(oi)(ci) low /t
icacls "C:\Users\<nextAccName>\Downloads" /setintegritylevel(oi)(ci) low /t
```

Ρύθμιση του Opera

Ένας ακόμα γνωστός φυλλομετρητής είναι ο Opera. Υπάρχει ένα WOT plugin και για αυτόν τον φυλλομετρητή.

Ρύθμιση σε Low Integrity του Opera

Μπορούμε να αυξήσουμε το επίπεδο ασφαλείας του υπολογιστή μας, ρυθμίζοντας τον Opera σε low integrity. Ανοίγουμε μία γραμμή εντολών (command prompt) με αυξημένα δικαιώματα, και εκτελούμε τις ακόλουθες εντολές, με τη σειρά, μια προς μια:

```
icacls "C:\program files (x86)\opera\opera.exe" /setintegritylevel low
icacls "C:\Users\sec web\AppData\Local\Opera Software" /setintegritylevel(oi)(ci)
low /t
icacls "C:\Users\sec web\AppData\Roaming\Opera Software"
/setintegritylevel(oi)(ci) low /t
```

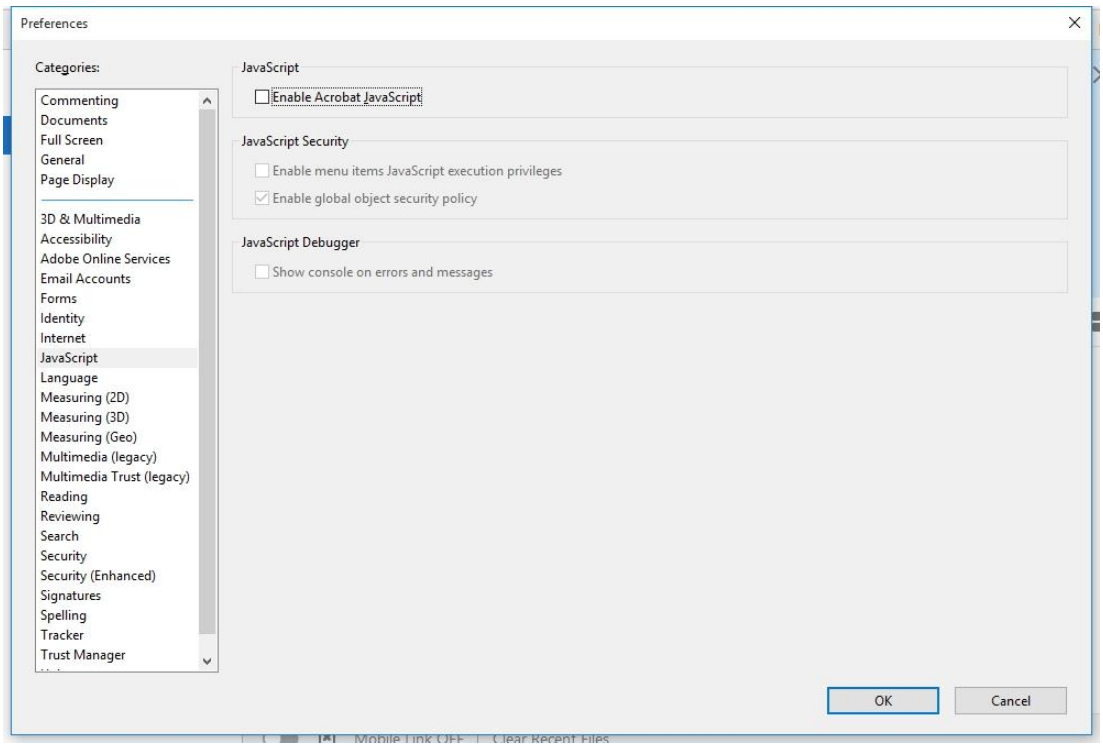
Ρύθμιση του Chrome

Ο Chrome είναι ο φυλλομετρητής της Google και είναι ένα λογισμικό ανοιχτού κώδικα. Η αρχιτεκτονική του επιτρέπει την τοποθέτηση των χαρακτηριστικών υψηλού κινδύνου, όπως HTML parser, JavaScript virtual

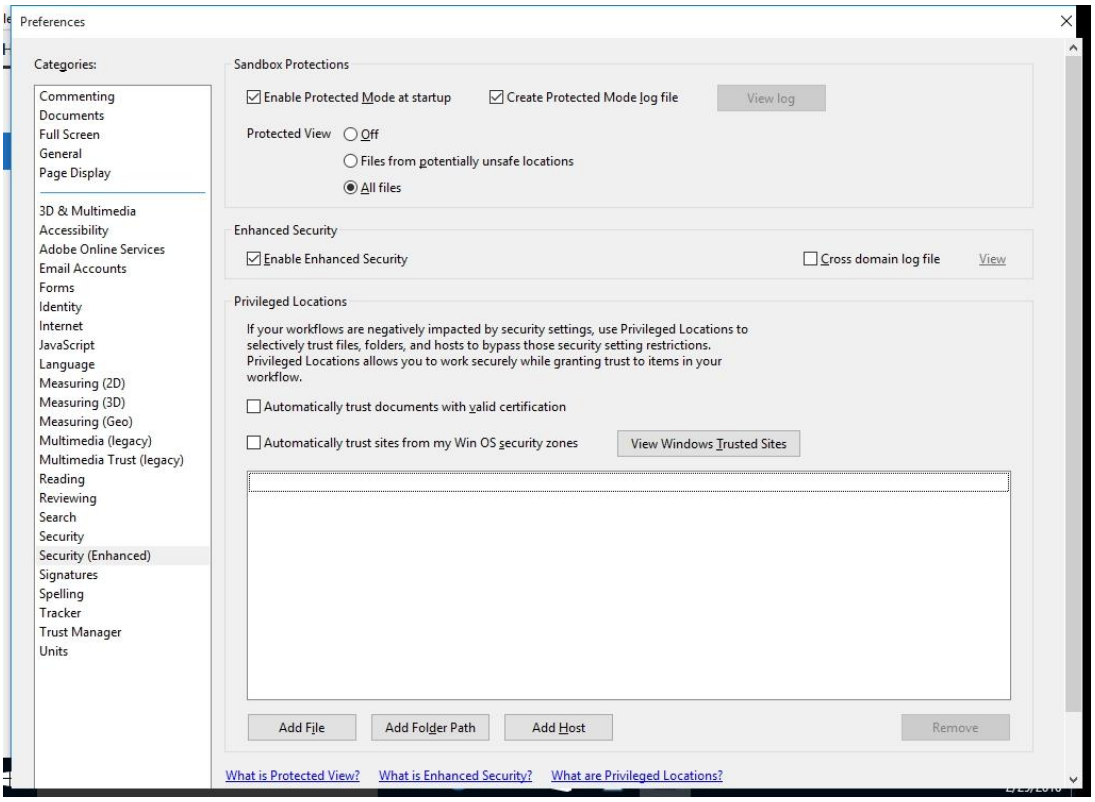
machine και το Document Object Model (DOM), σε περιβάλλον περιορισμένων δικαιωμάτων (sandboxed rendering engine). Δεν επιτρέπει τροποποιήσεις στο σύστημα των Windows. Αυτό το περιορισμένο περιβάλλον (sandbox), έχει σχεδιαστεί ώστε να παρέχει προστασία από κενά ασφαλείας, τα οποία προκύπτουν από έλλειψη ενημερώσεων. Επιπρόσθετα, χρησιμοποιεί την λειτουργία Protected Mode του IE σε Vista, Windows 7,8 και 10. Ο Chrome έχει ακόμα προσθέσει ένα περιορισμένο περιβάλλον σε ότι αφορά τον Adobe Flash, έτσι ώστε να αποτρέψει κενά ασφαλείας στον Flash, προκειμένου να μην παραβιαστεί το λειτουργικό σύστημα. Ο Chrome έχει τη δυνατότητα αυτόματης ενημέρωσης.

Ασφαλής ρύθμιση του Acrobat Reader

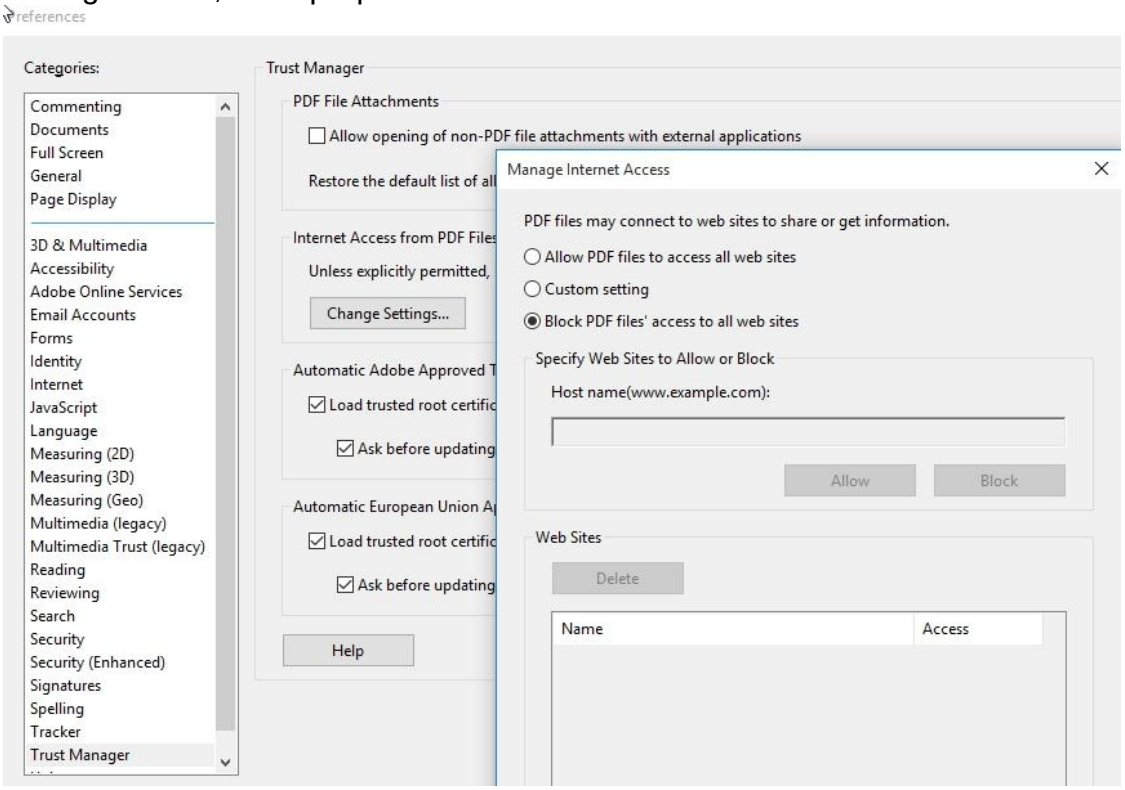
Εκτελούμε τον Acrobat Reader (εάν είναι εγκατεστημένος) για να ρυθμίσουμε την ασφάλειά του.Επιλέγουμε:
Edit > Preferences> Javascript, αποεπιλέγουμε "Enable Acrobat Javascript".



> Επιλέγουμε
Security Enhanced --> Protected View : All Files
> Security Enhanced: Create Protected Mode Log File.
> Security Enhanced: αποεπιλέγουμε Automatically Trust Sites from my Win OS Security Zones.



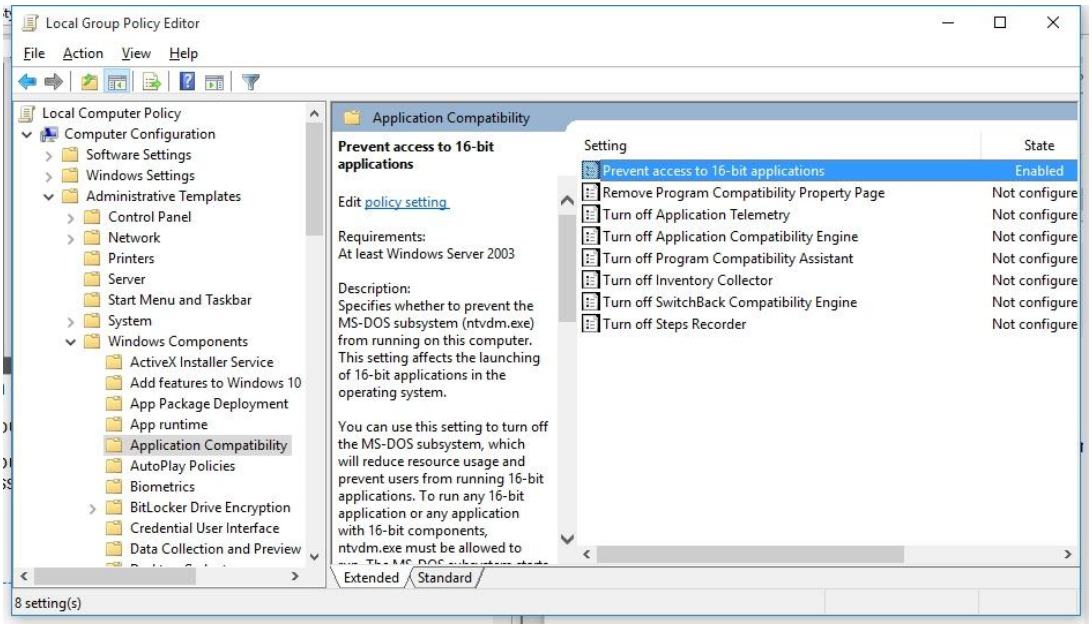
> Επιλεγουμε Trust Manager --> αποεπιλέγουμε Allow Opening of Non-PDF file attachments
>Trust Manager--> Internet Access from PDF outside the web browser Change Settings button, επιλέγουμε Block PDF file access to all web sites.



Απενεργοποίηση των 16 bit εφαρμογών (Turn off 16 bit apps)

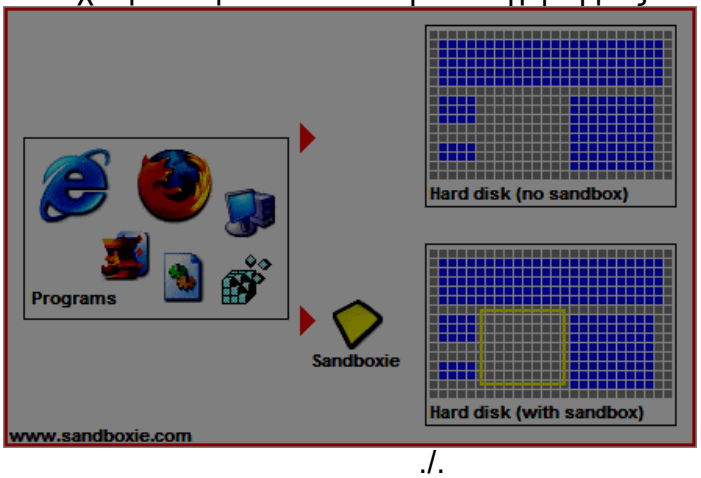
Είναι σημαντικό, εφόσον δεν χρησιμοποιούνται πλέον, να απενεργοποιήσουμε τις εφαρμογές 16 bit. Για να το κάνουμε αυτό, δίνουμε την εντολή 'gpedit.msc' και πάμε:

Computer config/administrative templates/windows components/app compatability/prevent access to 16 bit applications=enable



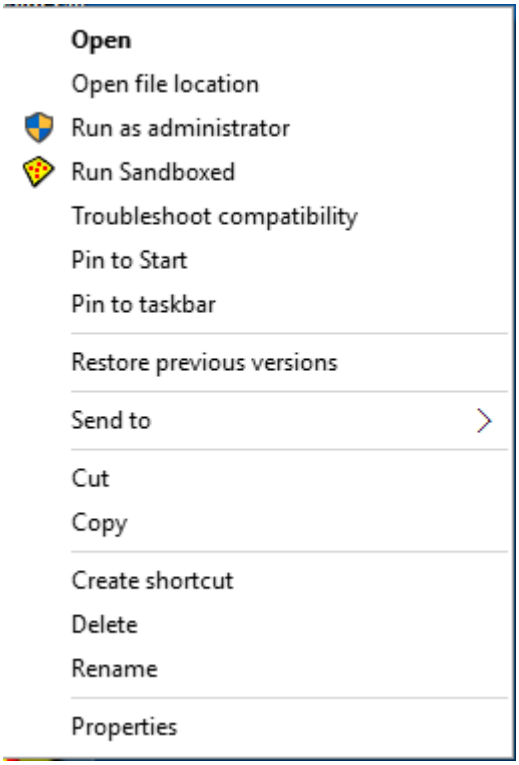
ΤΜΗΜΑ 13
ΠΩΣ ΕΚΤΕΛΟΥΜΕ ΜΙΑ ΑΓΝΩΣΤΗ ΕΦΑΡΜΟΓΗ

Στην περίπτωση που δεν είμαστε σίγουροι για κάποια εφαρμογή, μπορούμε να την “εκτελέσουμε” μέσα από ένα περιοριστικό περιβάλλον (sandbox), όπως το sandboxie (http://www.sandboxie.com/). Με αυτόν τον τρόπο πετυχαίνουμε να μην γίνουν μόνιμες αλλαγές / εγγραφές στον δίσκο μας και αν διαπιστώσουμε ότι πρόκειται για ιομορφικό λογισμικό, απλά κλείνουμε το sandboxie, χωρίς να σώσουμε τις αλλαγές. Με το sandbox, μπορούμε να “τρέξουμε” και τον browser μας και έτσι να έχουμε ασφάλεια κατά την πλοήγηση μας στο διαδίκτυο.



./.

Για να τρέξουμε μία εφαρμογή μέσα από το sandboxie κάνουμε δεξί κλικ στην εφαρμογή και επιλέγουμε **Run Sandboxed**

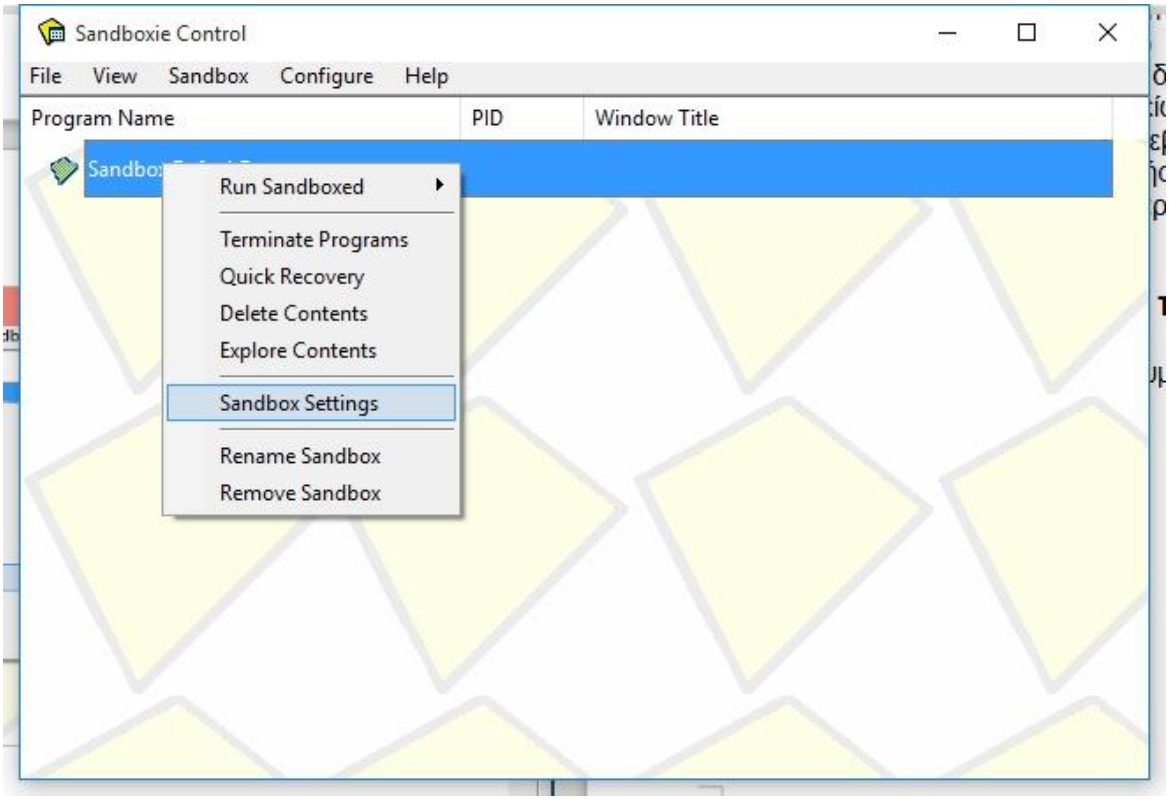


Περιοριστικό περιβάλλον εκτέλεσης φυλλομετρητών και άγνωστων προγραμμάτων

Όπως ήδη προαναφέρθηκε, υπάρχει ένα πρόγραμμα που καλείται Sandboxie (http://www.sandboxie.com/), το οποίο χρησιμοποιείται για την προστασία των φυλλομετρητών. Συγκεκριμένα, ο «προστατευμένος» φυλλομετρητής έχει πρόσβαση σε ένα μόνο συγκεκριμένο τμήμα του δίσκου. Το Sandboxie δεν αποτρέπει μια επίθεση, αλλά περιορίζει την επίθεση στο συγκεκριμένο τμήμα. Εάν η επίθεση δημιουργήσει αρχεία και φακέλους, αυτά θα δημιουργηθούν στο συγκεκριμένο τμήμα. Εάν γίνει εγκατάσταση ιομορφικών εργαλείων και λογισμικού, θα γίνει επίσης στο συγκεκριμένο μέρος του σκληρού. Όλα τα αρχεία που κατεβάζουμε (downloads), θα κατέβουν στο συγκεκριμένο τμήμα και από εκεί θα τα επιτρέψει το Sandboxie να μεταφερθούν πίσω στο κανονικό περιβάλλον. Τέλος οτιδήποτε υπάρχει στο συγκεκριμένο μέρος, μπορεί να ‘καθαριστεί’, με ένα απλό κλικ.

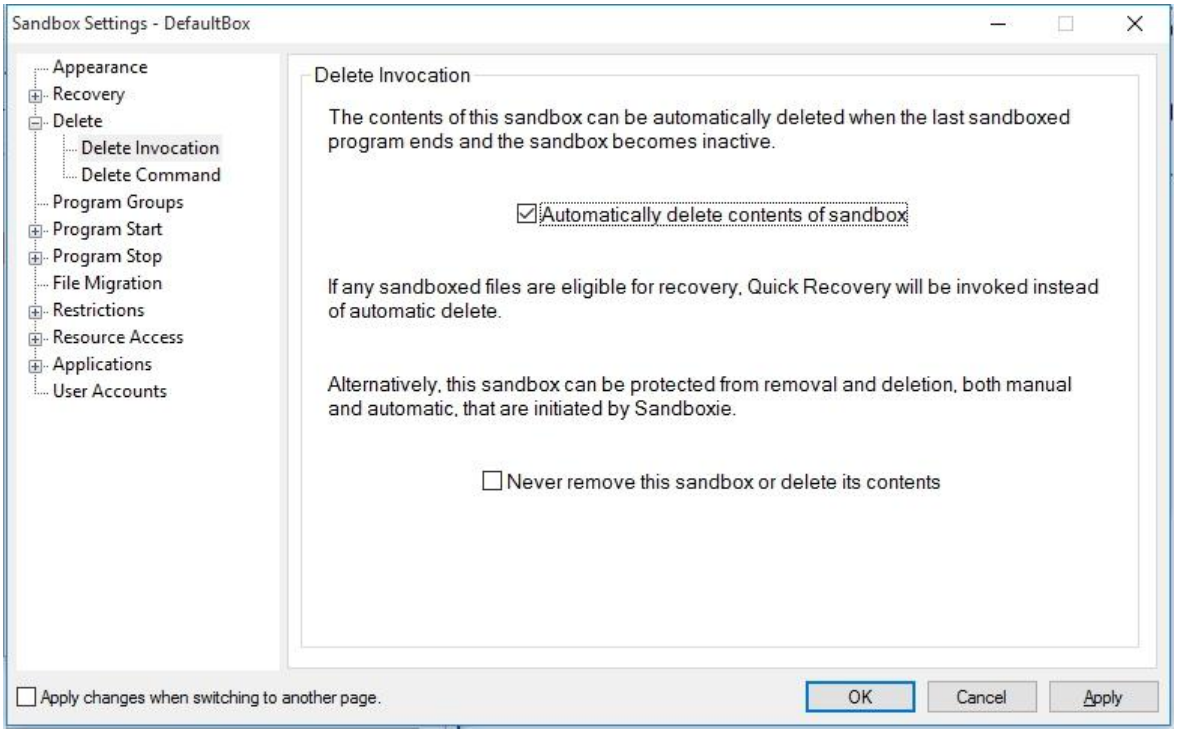
Ρύθμιση του περιοριστικού περιβάλλοντος

Δεξί κλικ στο sandbox και επιλέγουμε Sandbox Settings

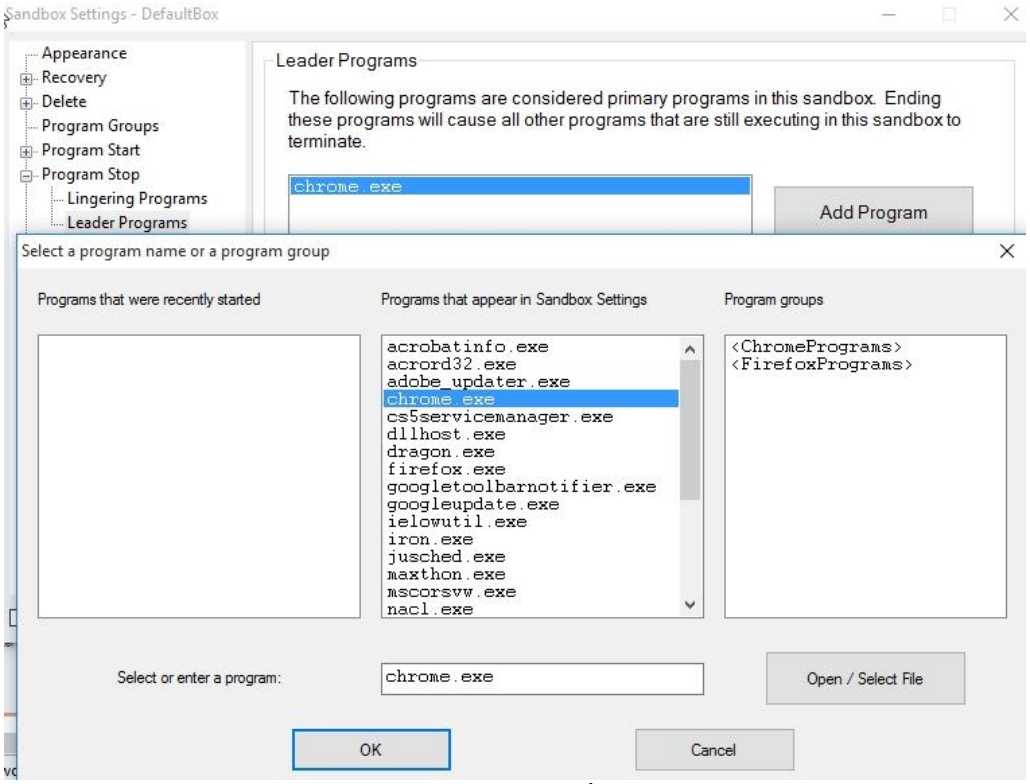


Για να ρυθμίσουμε το Sandboxie, έτσι ώστε οτιδήποτε περιορίζεται μέσα σε αυτό να μην μεταφέρεται στην συνέχεια στο συτημα, ενεργούμε ως εξής, πάμε στο:

delete->delete invocation> επιλέγουμε automatically delete contents of sandbox, έτσι ώστε οτιδήποτε φτάνει στο sandbox να μην παραμένει στο σύστημα



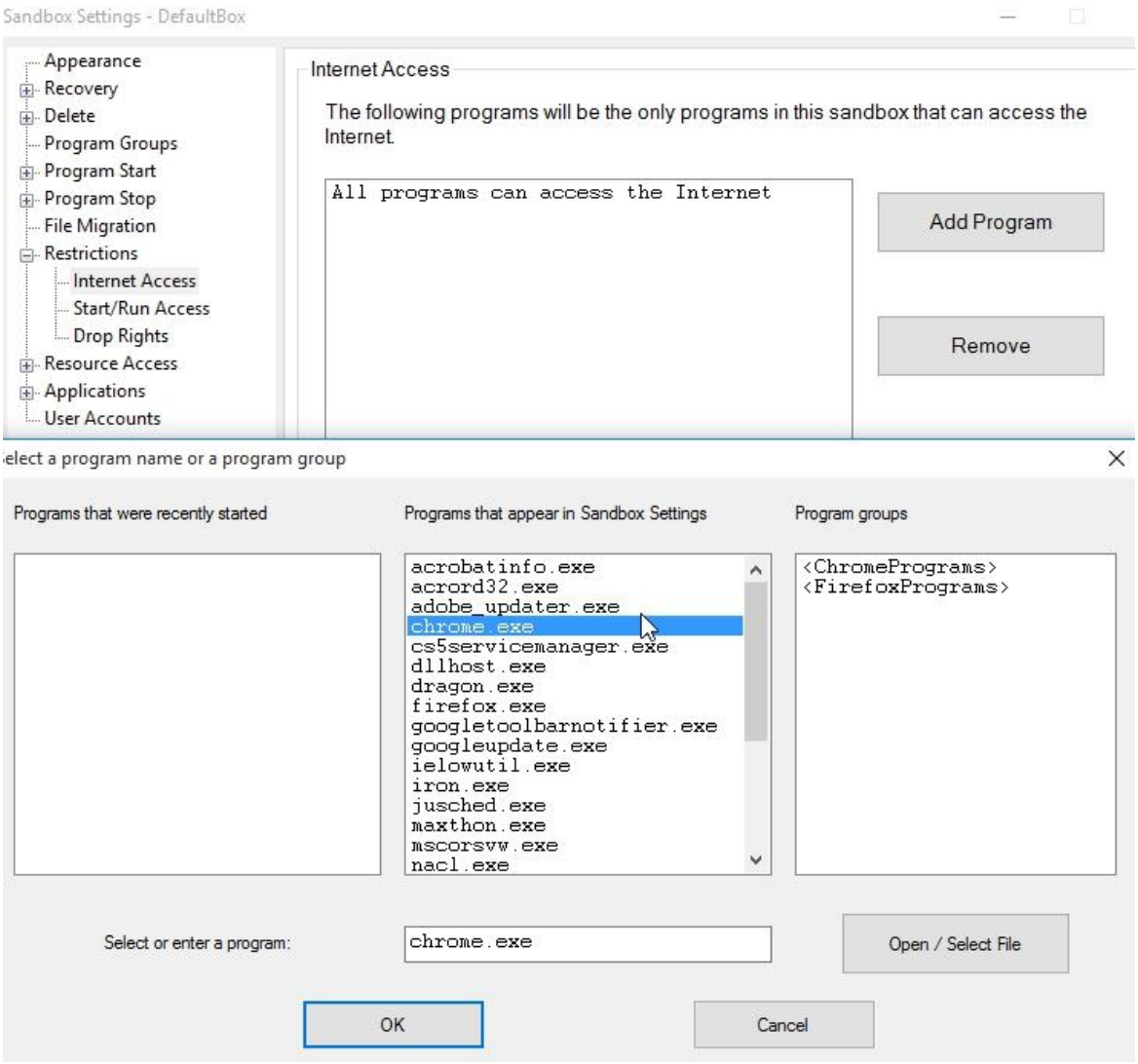
Για να ρυθμίσουμε το Sandboxie, έτσι ώστε οτιδήποτε περιορίζεται μέσα σε αυτό να μην μεταφέρεται στην συνέχεια στο σύστημα, αφού σταματήσει η εφαρμογή, παράδειγμα ο chrome ενεργούμε ως εξής, πάμε στο:
program stop->leader programs>add program > chrome
έτσι ώστε οτιδήποτε φτάνει στο sandbox να σταματά μόλις ο chrome σταματά



./.

Για να ρυθμίσουμε το Sandboxie, έτσι ώστε οτιδήποτε περιορίζεται μέσα σε αυτό να μην έχει πρόσβαση στο διαδίκτυο, παράδειγμα ο chrome να μην έχει πρόσβαση στο διαδίκτυο, ενεργούμε ως εξής, πάμε στο:

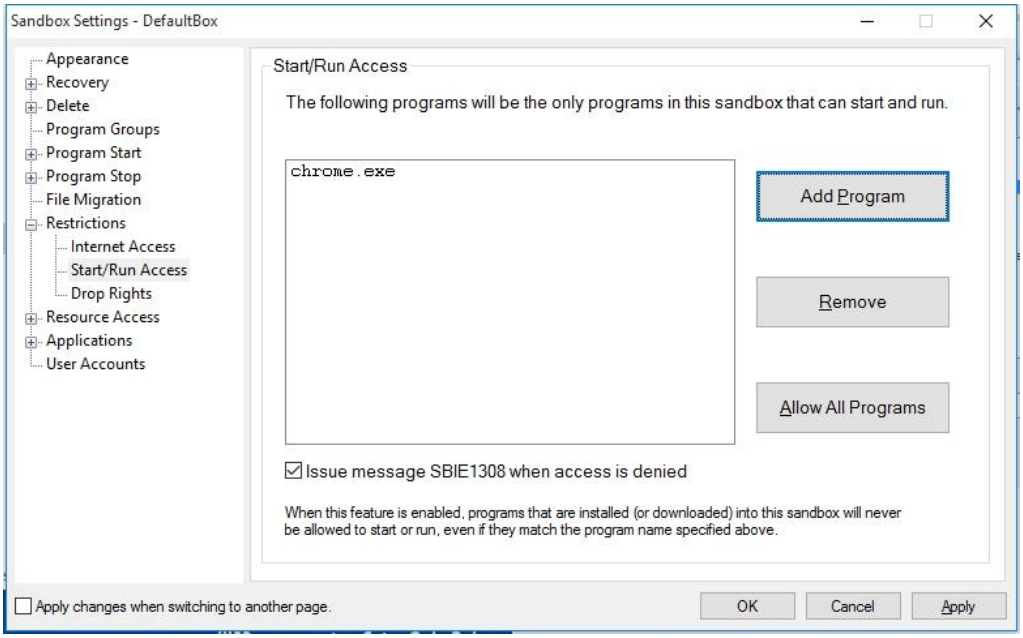
restrictions->Internet access> add programm > chrome
έτσι ώστε οτιδήποτε φτάνει στο sandbox να μην μπορεί να έχει πρόσβαση στο διαδίκτυο



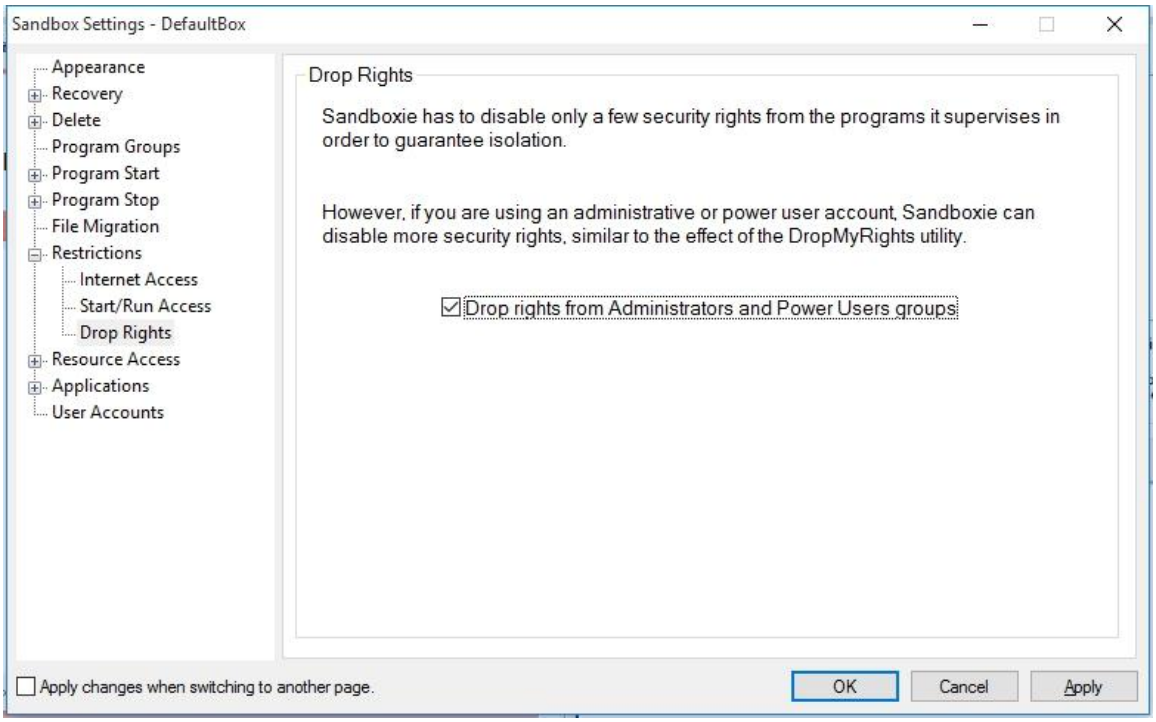
Για να ρυθμίσουμε το Sandboxie, έτσι ώστε μία εφαρμογή, παράδειγμα ο chrome να εκτελείται μέσα από το Sandboxie και μόνο αυτή όχι κάποια άλλη, παράδειγμα να μην εκτελείται το ιομορφικό λογισμικό, ενεργούμε ως εξής, πάμε στο:

restrictions->start/run access> only chrome

./.



Για να ρυθμίσουμε το Sandboxie, έτσι ώστε μία εφαρμογή, που εκτελείται μέσα Sandboxie, έχει περιορισμένα δικαιώματα, ενεργούμε ως εξής, πάμε στο: restrictions->drop rights> επιλέγουμε 'drop rights ...'



ΤΜΗΜΑ 14
ΠΩΣ ΜΠΛΟΚΑΡΟΥΜΕ ΠΡΟΓΡΑΜΜΑΤΑ ΜΕ LOW INTEGRITY ΔΙΚΑΙΩΜΑΤΑ ΩΣΤΕ ΝΑ ΜΗΝ ΑΠΟΚΤΗΣΟΥΝ ΠΡΟΣΒΑΣΗ ΣΤΑ ΕΓΓΡΑΦΑ ΜΑΣ

./.

Υπάρχει μια επιλογή, όπου τα low integrity προγράμματα μπορούν να ρυθμιστούν ώστε να μην μπορούν να διαβάσουν medium integrity τοποθεσίες. Αυτό ακριβώς κάνουν οι εντολές που ακολουθούν. Μόλις εκτελεστούν οι εντολές, η επιφάνεια εργασίας, τα έγγραφα, οι εικόνες, τα βίντεο και οι φάκελοι μουσικής δεν θα είναι αναγνώσιμοι (unreadable), από οποιοδήποτε πρόγραμμα, το οποίο ανήκει στα low integrity. Η τελευταία εντολή, τροποποιεί τον φάκελο Downloads, έτσι ώστε να αλλάξει σε low integrity. Αυτό είναι απαραίτητο διότι χρειάζεται ένα μέρος όπου θα αποθηκεύονται τα downloads. Θα δημιουργήσουμε και ένα Upload directory, όπου θα αντιγράφουμε εκεί το αρχείο το οποίο θέλουμε να ανεβάσουμε. Ο Upload folder δεν έχει επεξεργαστεί από chml, συνεπώς ο low integrity φυλλομετρητής μπορεί να διαβάσει αυτό το φάκελο. Όλα αυτά μας προστατεύουν από low integrity programs όπως ο IE.

Πάμε στο --> http://www.minasi.com/apps/ για να κατεβάσουμε το chml.exe

Ανοίγουμε μία γραμμή εντολών (command prompt) με δικαιώματα διαχειριστού (Administrator). Πάμε search, γράφουμε cmd.exe και στο menu που μας εμφανίζεται κάνουμε δεξί κλικ στο cmd και επιλέγουμε 'run as administrator και εκτελούμε τις ακόλουθες εντολές :

cd "\user\<yourAccName>\downloads\chml"ή οπουδήποτε έχουμε αποθηκεύσει το chml)
chml "c:\users\<yourAccName>\desktop"-i:m -nr -nw –nx
chml "c:\users\<yourAccName>\documents"-i:m -nr -nw –nx
chml "c:\users\<yourAccName>\pictures"-i:m -nr -nw –nx
chml "c:\users\<yourAccName>\videos"-i:m -nr -nw –nx
chml "c:\users\<yourAccName>\music"-i:m -nr -nw –nx
chml "c:\users\<yourAccName>\downloads" -i:l

ΤΜΗΜΑ 15
ΑΣΦΑΛΕΙΑ ΚΑΤΑ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΝΕΟΥ ΛΟΓΙΣΜΙΚΟΥ

Όταν χρειάζεται να κάνουμε εγκατάσταση νέου λογισμικού, πολλές φορές απαιτείται και σύνδεση στο διαδίκτυο, προκειμένου να κατεβάσουμε κάποια δεδομένα. Επίσης, ίσως δημιουργηθεί ένα εκτελέσιμο, μέσα στον φάκελο temp, έτσι ώστε να πραγματοποιηθεί το κατέβασμα του αρχείου που θέλουμε να εγκαταστήσουμε και το εκτελέσιμο σβήνεται αυτόματα μόλις τελειώσει η εγκατάσταση. Σε αυτή την περίπτωση, ίσως να μην είναι δυνατό να δημιουργήσουμε έναν κανόνα outbound allow, για αυτό το εκτελέσιμο. Συνεπώς, η μόνη λύση είναι να πάμε στο Windows Firewall with Advanced Security και να θέσουμε προσωρινά Outbound to allow for the Public profile. Τέλος, όταν τελειώσει η εγκατάσταση του νέου προγράμματος, θέτουμε πάλι Outbound block.

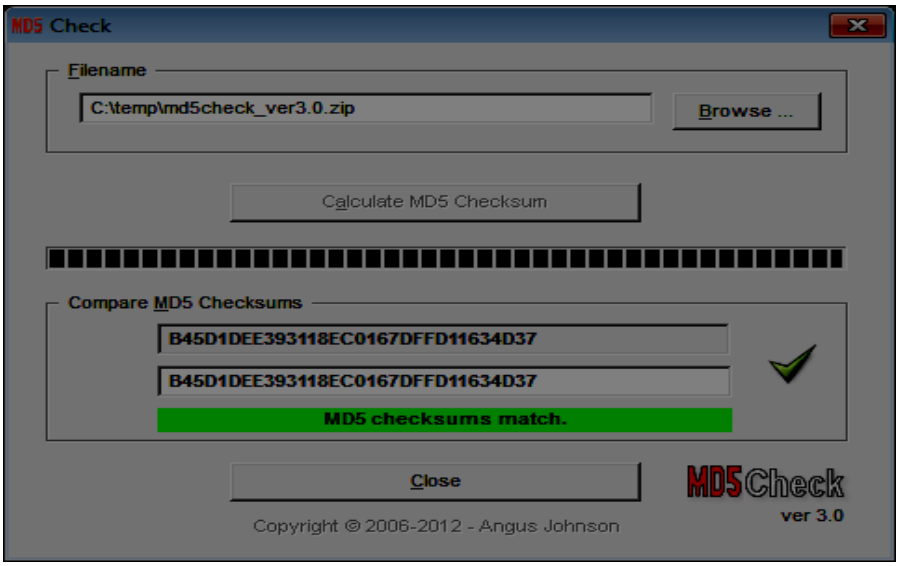
Σημείωση: Εάν η εφαρμογή είναι διαδικτυακή ή λαμβάνει δεδομένα από αρχεία που κατέβηκαν από το διαδίκτυο (internet), τότε την «προσθέτουμε» στο EMET.

ΤΜΗΜΑ 16

ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΕΛΕΓΧΟΥ ΑΚΕΡΑΙΟΤΗΤΑΣ

Για να είμαστε σίγουροι ότι το αρχείο που μεταφορτώσαμε (download) είναι όντως αυτό που θέλουμε και δεν έχει υποστεί κανενός είδους ψηφιακή αλλοίωση (επισύναψη ιομορφικού λογισμικού), θα πρέπει ο πάροχος του αρχείου να μας δίνει την τιμή του ελέγχου ακεραιότητας του, μαζί με τον αλγόριθμο που χρησιμοποίησε για την εξαγωγή αυτής της τιμής.

Έτσι, αφού κατεβάσουμε το αρχείο στον υπολογιστή μας και ανάλογα με τον αλγόριθμο που χρησιμοποίησε ο πάροχος του αρχείου, τότε και εμείς θα πρέπει να χρησιμοποιήσουμε τον αντίστοιχο αλγόριθμο για επιβεβαίωση της σωστής τιμής ακεραιότητας. Για md5 μπορούμε παράδειγμα να χρησιμοποιήσουμε το MD5 Check (**http://angusj.com/delphi/md5check_setup.exe**) και ελέγχουμε με αυτό την ακεραιότητα του αρχείου που μεταφορτώσαμε (download). Ένα άλλο εργαλείο γραμμής εντολών της Microsoft είναι και το Microsoft File Checksum Integrity Verifier. Άλλα εργαλεία είναι και το md5deep και το hashdeep (http://md5deep.sourceforge.net/).



Αλγόριθμοι ελέγχου ακεραιότητας είναι οι md5, sha1, sha256, sha512, pgp και άλλοι. Στην παρακάτω εικόνα φαίνεται ένα παράδειγμα, με χρήση του sha1.

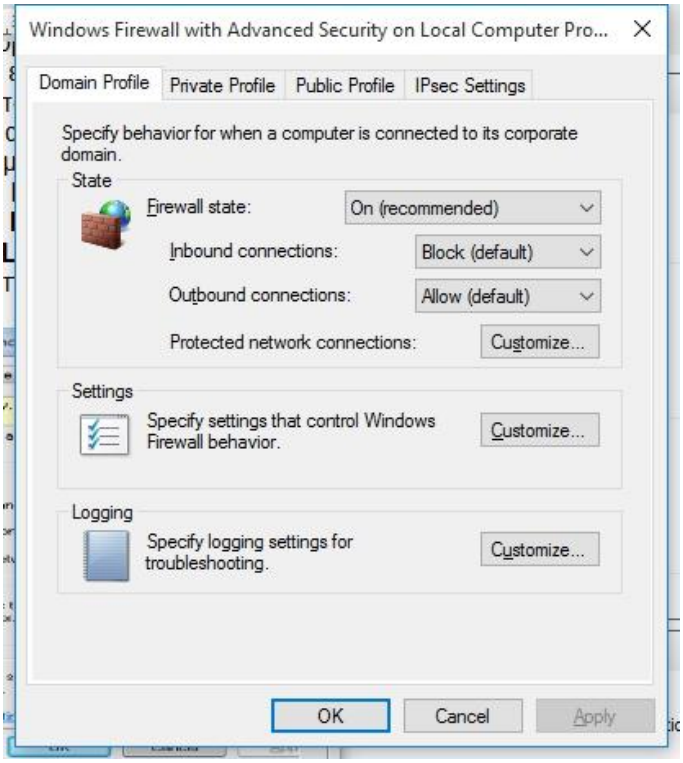
Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	2.9G	**2016.2**	25cc6d53a8bd8886fcb468eb4fbb4cdfac895c65
Kali Linux 32 bit	ISO	Torrent	2.9G	**2016.2**	9b4e167b0677bb0ca14099c379e0413262eefc8c
Kali Linux 64 bit Light	ISO	Torrent	1.1G	**2016.2**	f7bdc3a50f177226b3badc3d3eafcf1d59b9a5e6
Kali Linux 32 bit Light	ISO	Torrent	1.1G	**2016.2**	3b637e4543a9de7ddc709f9c1404a287c2ac62b0
Kali Linux 64 bit e17	ISO	Torrent	2.7G	**2016.2**	4e55173207aef7ef584661810859c4700602062a
Kali Linux 64 bit Mate	ISO	Torrent	2.8G	**2016.2**	bfaeaa09dab907ce71915bcc058c1dc6424cd823
Kali Linux 64 bit Xfce	ISO	Torrent	2.7G	**2016.2**	e652ca5410a44e4dd49e120befdace38716b8980
Kali Linux 64 bit LXDE	ISO	Torrent	2.7G	**2016.2**	d8eb6e10cf0076b87abb12eecb70615ec5f5e313
Kali Linux armhf	Image	Torrent	0.7G	**2016.2**	7aec28a2aa7f303467d29d7e3cf38fd372aefe4c
Kali Linux armel	Image	Torrent	0.7G	**2016.2**	6b90d5a7f8d2627016e63caf5b895f7ca814c6c0

ΤΜΗΜΑ 17
ΡΥΘΜΙΣΗ ΤΩΝ ΜΗΤΡΩΝ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ (EVENT LOG FILES)

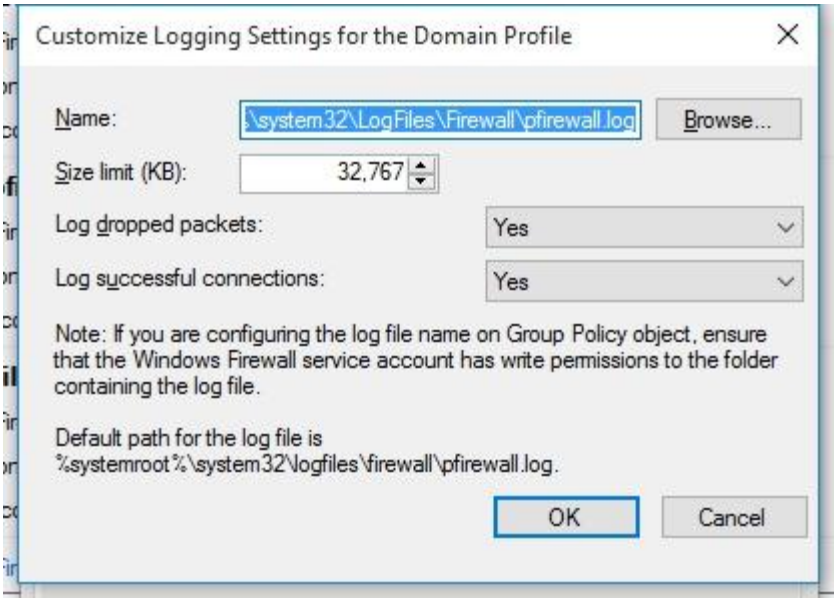
Ενεργοποίηση των μητρώων καταγραφής συμβάντων (Event Log files)

Στα Windows 10 υπάρχουν log files, στα οποία καταγράφονται πληροφορίες για το σύστημα (System log files), για τις εφαρμογές (Application log), για την ασφάλεια (Security log). Ωστόσο, δεν είναι ενεργοποιημένα εξ' ορισμού. Για να τα ενεργοποιήσουμε, ώστε μελετώντας τα να μπορούμε να εντοπίσουμε προσπάθειες εκμετάλλευσης του συστήματός μας από κακόβουλους χρήστες, όπως πχ επιθέσεις brute forcing (επίθεση ανάκτησης συνθηματικού), κάνουμε τα εξής:

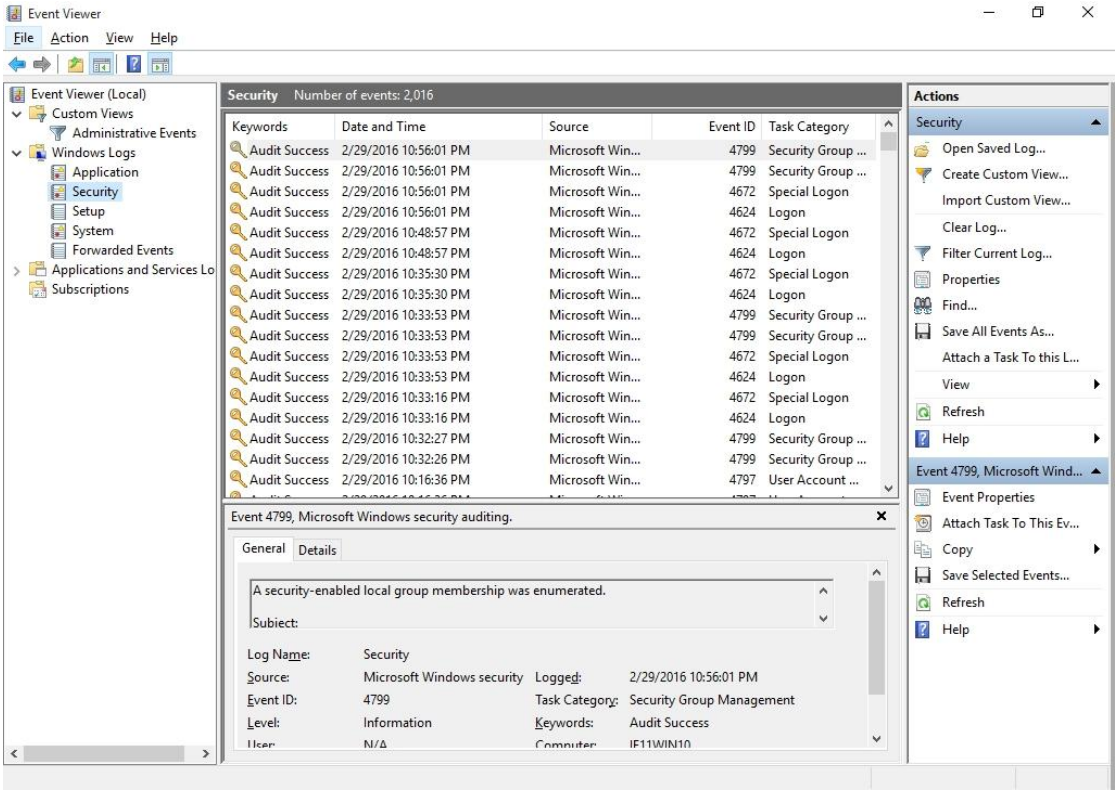
Στο **Search** , ή πατώντας το windows button, στη γραμμή αναζήτησης πληκτρολογούμε **wf.msc** για να ανοίξουμε το **Windows Firewall with Advanced Security**. Στο **Windows Firewall With Advanced Security on Local Computer** κάνουμε δεξί κλικ και επιλέγουμε **Properties** για να ανοίξει το παρακάτω παράθυρο.



Επιλέγουμε **customize** στο πεδίο **Logging.** Στο νέο παράθυρο μπορούμε να καθορίσουμε την τοποθεσία αποθήκευσης των Log files καθώς και το μέγεθος του αρχείου. Για την ενεργοποίηση του logging επιβεβαιώνουμε ότι η επιλογή στα δύο drop down menus (Log dropped packets & Log Successful connections) είναι στο **Yes.** Στη συνέχεια πατάμε **OK** δύο φορές.



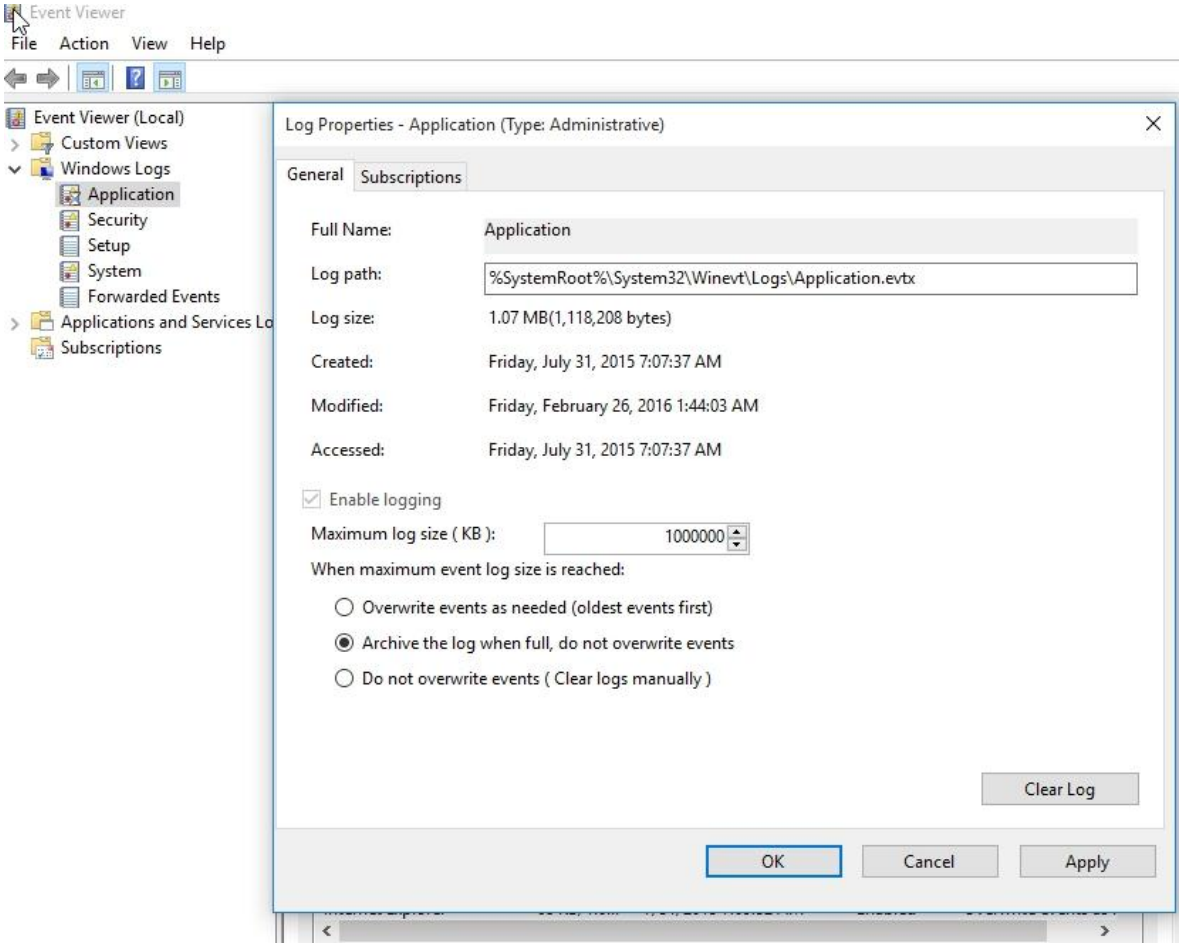
Για να παρακολουθήσουμε τις εγγραφές (log entries) στο μητρώο καταγραφής συμβάντων, χρησιμοποιούμε το πρόγραμμα Event Viewer. Επιλέγουμε **start** και πληκτρολογούμε **event viewer**.



Αύξηση μεγέθους καταγραφής των μητρώων καταγραφής συμβάντων (Event Log files)

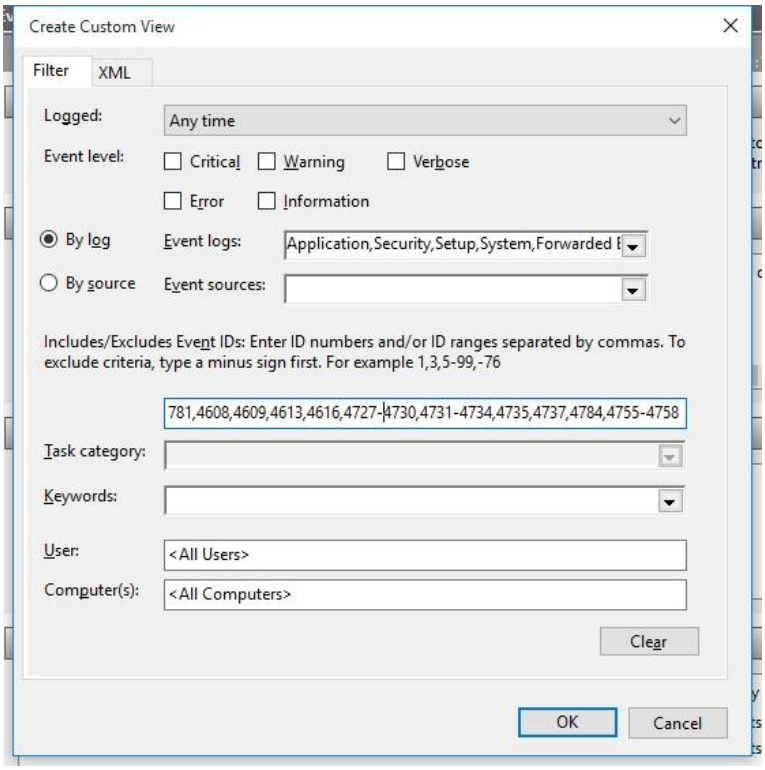
Πολλές φορές δεν είναι δυνατό να ανακαλύψουμε από την πρώτη μέρα ότι έχουμε δεχτεί επίθεση. Συχνά, η ανακάλυψή της προκύπτει αρκετές εβδομάδες ή και μήνες αργότερα. Συνεπώς θα χρειαστεί να διατηρήσουμε τις εγγραφές των μητρώων καταγραφής συμβάντων (log entries), για μήνες, ωστόσο το προκαθορισμένο μέγεθος των αρχείων καταγραφής είναι πολύ μικρό. Για να αλλάξουμε το μέγεθος καταγραφής των μητρώων και να το αυξήσουμε στο μέγιστο, πάμε στο:

Control Panel/Administrative Tools /Event Viewer
Κάνουμε δεξί κλικ Application, Properties και θέτουμε log size to 1000000. Κάνουμε το ίδιο για 'Security' και 'System'.



Περιστατικά ασφαλείας προς παρακολούθηση (Security Events to Monitor for)

Έχουμε την δυνατότητα να δημιουργήσουμε και φίλτρα, στα μητρώα καταγραφής συμβάντων, ώστε να παρακολουθούμε συγκεκριμένες δραστηριότητες στον υπολογιστή μας. Για να το πετύχουμε αυτό, δημιουργούμε Custom Views για τα ακόλουθα Event logs, με τον ακόλουθο τρόπο:
Επιλέγουμε 'Create Custom View'. Επιλέγουμε 'By Log', pull down 'Event Logs', Επιλέγουμε 'Windows Logs', πάμε στο field <All Event IDs> και κάνουμε αντιγραφή και επικόλληση στο event id numbers, επιλέγουμε OK και δίνουμε όνομα στο view.



Σημαντικά events που πρέπει να παρακολουθούμε είναι και τα παρακάτω:

4723,4724 - Change Password
4720,4726,4738,4781 - Delete, Change Accounts
4608,4609 - Startup, Shutdown
4613 - Clear Security Log
4616 - Change System Time
4617 - Unable to Log
4714,4705 - Privilege assigned or removed
4708,4714 - Change audit policy
4717,4718 - System access granted or removed
4739 - Change domain policy
16390 - Administrator account lockout
4727-4730,4731-4734,4735,4737,4784,4755-4758 - Group changes
4624,4636,4803,4801 - Account logons
4672 - Admin account logons
4698 - Schedule new job
4656 - Access refused to object
3004,3005 - Windows defender finds something
4664 - Create hard link to audited file
865 - Software restriction triggered
1037 - Protected Mode violation
7031 - Service terminated unexpectedly
4697 - Install a Service
4663 - Access audited file

Τα παραπάνω 'custom view' φίλτρα βρίσκονται στο φάκελο "Event Viewer Custom Views". Απλά επιλέγουμε 'Import Custom View', έτσι ώστε να εισάγει κάθε xml αρχείο ένα προς ένα.

ΤΜΗΜΑ 18
ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ-ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΥΒΕΡΝΟ-ΠΕΡΙΣΤΑΤΙΚΩΝ

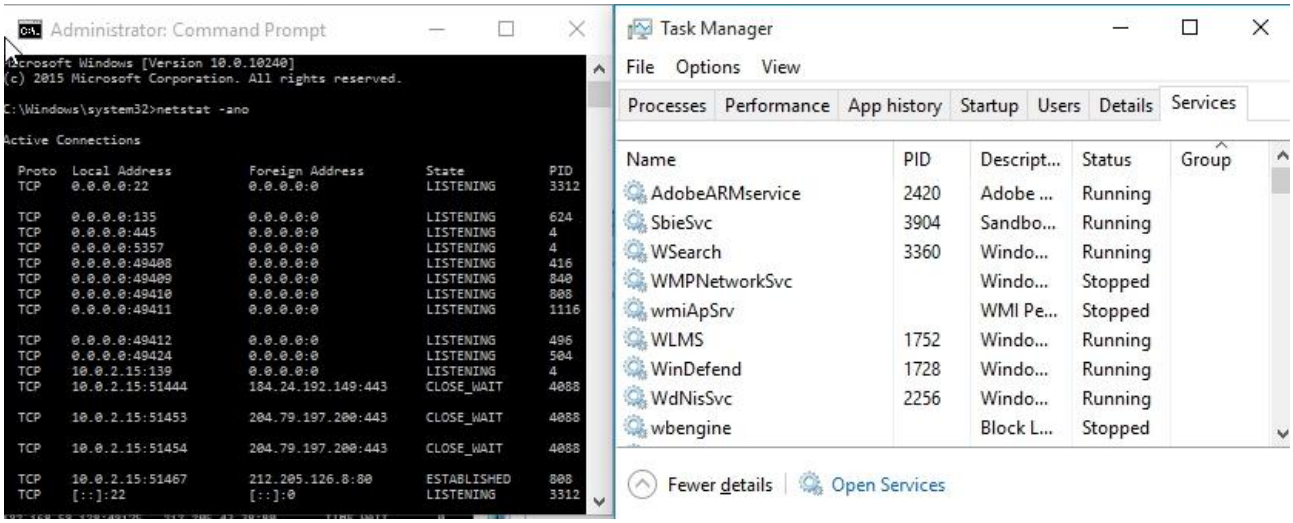
Εντοπισμός / καταγραφή ενεργών συνδέσεων

Για να δούμε τις συνδέσεις που πραγματοποιούμε στο διαδίκτυο ακολουθούμε την παρακάτω διαδικασία:

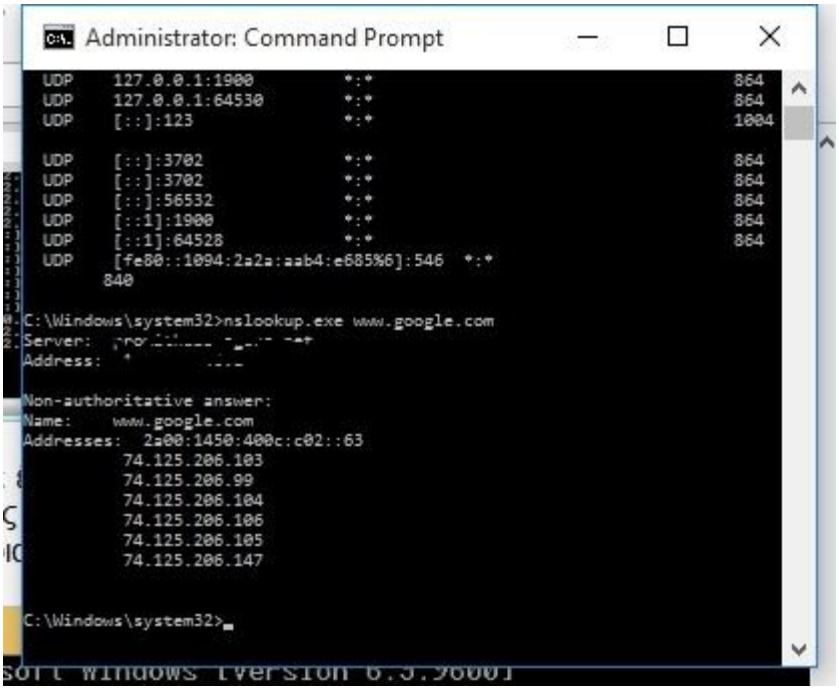
Στο **Search** , ή πατώντας το windows button, στη γραμμή αναζήτησης πληκτρολογούμε **cmd.exe** και πατάμε **enter**. Στη γραμμή εντολών (τερματικό) δίνουμε την εντολή:

c:\> **netstat -ano.**

Μπορούμε να ανοίξουμε τον **task manager** με τον συνδυασμό των πλήκτρων **ctrl+alt+del**. Θα έχουμε την παρακάτω εικόνα.



Μπορούμε έτσι να διακρίνουμε πιο πρόγραμμα κάνει ποιες συνδέσεις. Κάνοντας χρήση της εντολής nslookup στην γραμμή εντολών, μπορούμε να δούμε την αντιστοιχία domain names και IP, όπως διακρίνεται στην παρακάτω εικόνα:

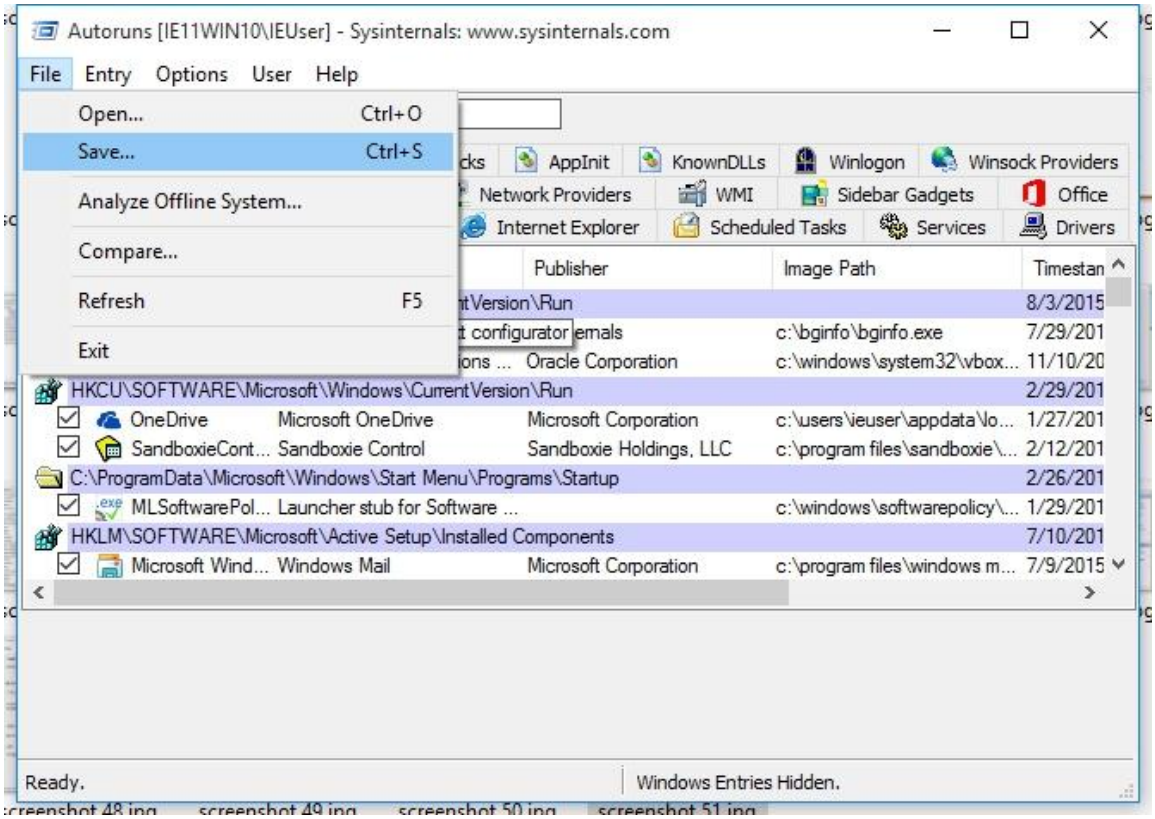


Είναι σημαντικό να προσέξουμε που συνδεόμαστε. Στην περίπτωση που μία IP αντιστοιχεί σε κάποιο ύποπτο ιστότοπο, τότε το πρόγραμμα/υπηρεσία που έχει κάνει τη σύνδεση είναι ιομορφικό.

Εντοπισμός /καταγραφή των διεργασιών (Process Explorer - AutoRuns)

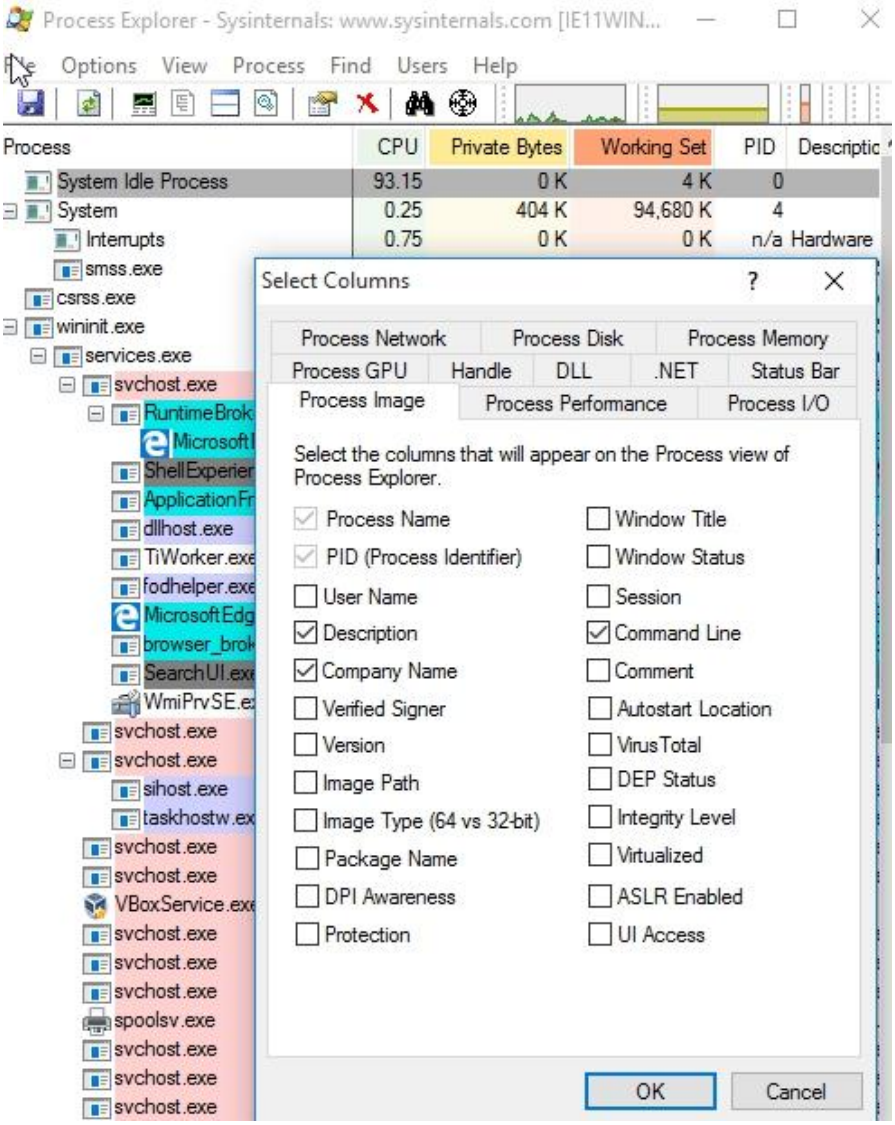
Εάν θέλουμε να γνωρίζουμε τι προγράμματα τρέχουν στον υπολογιστή μας, έτσι ώστε να είμαστε σίγουροι ότι δεν περιέχουν κάποιο spyware ή άλλα ιομορφικά λογισμικά, μπορούμε να χρησιμοποιήσουμε δύο (2) εφαρμογές που έχουν αυτή την δυνατότητα. Το ένα από αυτά είναι το AutoRuns, και είναι διαθέσιμο εδώ : http://technet.microsoft.com/en-us/sysinternals/bb963902

Κατεβάζουμε το αρχείο, το κάνουμε unzip, δημιουργούμε ένα φάκελο στο \Program Files (x86) και αντιγράφουμε όλα τα αρχεία του εδώ. Το AutoRuns παρέχει μια λίστα με όλα τα σημεία στη registry, όπου τα προγράμματα τρέχουν αυτόματα. Κάνουμε δεξί κλικ σε αυτό,επιλέγουμε Run as admin, και χρησιμοποιούμε File/Save για να πάρουμε ένα snapshot από τις τρέχουσες ρυθμίσεις του υπολογιστή. Αργότερα, όταν θέλουμε να εφαρμόσουμε ελέγχους στον υπολογιστή μας, μπορούμε να χρησιμοποιήσουμε αυτό το snapshot, και να το συγκρίνουμε με τις τρέχουσες ρυθμίσεις, προκειμένου να ανακαλύψουμε εάν έχει αλλάξει κάτι. Τα New entries εμφανίζονται με πράσινο χρώμα. Εάν όλα τα πράσινα entries είναι ‘καλά’, τότε σώζουμε το αρχείο ξανά με τις τρέχουσες ρυθμίσεις.



Το δεύτερο πρόγραμμα είναι ο Process Explorer, και είναι διαθέσιμος εδώ:
http://technet.microsoft.com/en-us/sysinternals/bb896653
Το πρόγραμμα αυτό είναι όπως ο Task Manager, αλλά εμφανίζει περισσότερες πληροφορίες. Πολλά κακόβουλα λογισμικά, ονομάζουν τον εαυτό τους με γνωστά ονόματα προγραμμάτων των Windows, προσπαθώντας έτσι να κρυφτούν. Κάνουμε δεξί κλικ στο πρόγραμμα και επιλέγουμε 'run as admin', πάμε στο View/Select Columns και επιλέγουμε ‘command line’. Μετά File/Save. Το αρχείο κειμένου που προκύπτει είναι τώρα ένα snapshot που περιέχει ότι τρέχει υπό κανονικές συνθήκες, όταν κάνουμε για πρώτη φορά login.

Στη συνέχεια, κάνουμε μια επανεκκίνηση του υπολογιστή και ανοίγουμε έναν command prompt με αυξημένα δικαιώματα ('run as admin'), και πληκτρολογούμε :
netstat -abn > netstat-baseline.txt
Το πρόγραμμα netstat εμφανίζει μια λίστα από προγράμματα που ακούμε και συνδέονται στο δίκτυο. Εάν ένας επιτιθέμενος συνδέεται στον υπολογιστή μας, το πρόγραμμα του θα συνδέεται από τον υπολογιστή μας, στον υπολογιστή του, και το πρόγραμμα θα εμφανίζεται σε αυτή τη λίστα.



Τελευταία έχουμε την επιλογή να τρέξουμε το “**sfc /scannow**”, προκειμένου να αποφασίσουμε αν έχει τροποποιηθεί κάποιο από τα αρχεία συστήματος. Το SFC περιέχει τις σωστές υπογραφές αρχείων των windows και κάνει μια σύγκριση με τις τρέχουσες ρυθμίσεις. Τέλος διορθώνει το πρόβλημα

ΤΜΗΜΑ 19
ΕΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΠΡΟΣΩΠΙΚΟ ΜΑΣ ΥΠΟΛΟΓΙΣΤΗ

Μπορούμε να πραγματοποιήσουμε έλεγχο ασφαλείας στον προσωπικό μας υπολογιστή με την χρήση του δωρεάν λογισμικού Microsoft Baseline Security Analyzer (MBSA). Έτσι θα έχουμε μία εικόνα του πόσο ενήμερος είναι ο υπολογιστής μας και τυχόν αδυναμίες που μπορεί να έχει και θα πρέπει να τις εξαλείψουμε.
Σχετικό link: http://technet.microsoft.com/en-us/security/cc184924
Το MBSA είναι δωρεάν λογισμικό για administrators, security auditors, και IT professionals και πραγματοποιεί security και vulnerability assessment ανιχνεύσεις.

./.

ΤΜΗΜΑ 20
ΓΙΑ ΠΡΟΧΩΡΗΜΕΝΟΥΣ ΧΡΗΣΤΕΣ

Οι πιο έμπειροι χρήστες μπορούν, για ακόμα μεγαλύτερη ασφάλεια, να χρησιμοποιούν και τις παρακάτω μεθόδους, συνδυαστικά.

Χρήση του εικονικού λειτουργικού συστήματος

Με την χρήση του Virtual box, μπορούμε να εκτελούμε ένα λειτουργικό σύστημα μέσα σε ένα άλλο. Μπορούμε δηλαδή μέσα σε ένα Windows 10 λειτουργικό σύστημα να “τρέξουμε” μέσα από το virtual box ένα άλλο Windows 10, το οποίο χρησιμοποιούμε για να σερφάρουμε στο διαδίκτυο. Αν μολυνθεί, απλά χρησιμοποιούμε ένα αντίγραφο το οποίο έχουμε δημιουργήσει στην αρχή, ή κάνουμε την χρήση του snapshot.
https://www.virtualbox.org/wiki/Downloads

ΤΜΗΜΑ 21
ΕΠΙΛΟΓΟΣ

Στην ασφάλεια υπάρχει ένας κανόνας, **δεν υπάρχει απόλυτη ασφάλεια**. Για αυτό θα πρέπει να γνωρίζουμε καλά την χρήση του υπολογιστή μας, την χρήση του διαδικτύου και να επαγρυπνούμε συνεχώς. Μόνο με συνεχή ενημέρωση και επαγρύπνηση έχουμε ένα επιθυμητό επίπεδο ασφάλειας. Η ασφάλεια είναι αποτέλεσμα εκπαίδευσης - ενημέρωσης, εφαρμογής διαδικασιών και χρήσης κατάλληλης υποδομής και λογισμικού. Βασικός κανόνας είναι να χρησιμοποιούμε μόνο **νόμιμο λογισμικό**. Το ασφαλέστερο λειτουργικό είναι αυτό που γνωρίζουμε καλύτερα και μπορούμε να τα παραμετροποιήσουμε εύκολα. Συνεπώς θα πρέπει να έχουμε μία προσωπική πολιτική ασφαλείας και να την εφαρμόζουμε στην καθημερινή μας εργασία.

Οι οδηγίες που παρουσιαστήκαν στον συγκεκριμένο οδηγό, έχουν σαν σκοπό να μειωθεί η επιθετική επιφάνεια, να εφαρμοστεί ο κανόνας των ελαχίστων προνομίων στον προσωπικό μας υπολογιστή. Παράλληλα δίνει την δυνατότητα να γνωρίσουμε καλύτερα το λειτουργικό και τις δυνατότητές του.

Αυτό που πρέπει τέλος να γνωρίζουμε είναι πως εμείς είμαστε υπεύθυνοι για την ασφάλεια του υπολογιστή μας και όχι κάποιο λογισμικό ή κάποιος τρίτος. Θα πρέπει η ασφάλεια να γίνει συνήθεια και να εκπαιδευόμαστε τακτικά μένοντας πάντα ενήμεροι για τους κινδύνους που διατρέχουμε όταν συνδεόμαστε στο διαδίκτυο.