ΕΠ ΚτΠ
Χρηματοδότηση:
Ευρωπαϊκό Κοινωνικό Ταμείο: 75%
Εθνικοί Πόροι: 25%

Εκπαιδευτικό Υλικό για την

Εγκατάσταση συνοδευτικού λογισμικού σε ΣΕΠ και υποστήριξή του (Windows2003/XP)

(Spybot Search & Destroy)

Ανάδοχος: Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών

Σεπτέμβριος 2008

Αναπτύχθηκε στο πλαίσιο υλοποίησης του Υποέργου 2
«Πρακτική Εκπαίδευση Εκπαιδευτικών Πληροφορικής»
της Πράξης «Δράσεις Επιμόρφωσης Εκπαιδευτικών Πληροφορικής»
της Κατηγορίας Πράξεων 1.2.2
«Επιμόρφωση εκπαιδευτικών και Πιστοποίηση»
του Μέτρου 1.2
«Εισαγωγή και Αξιοποίηση των Νέων Τεχνολογιών στην Εκπαίδευση»

Περιεχόμενα

1 Spybot Search & Destroy

Ένα από τα καλύτερα προγράμματα για τον έλεγχο και καθαρισμό των σταθμών εργασίας και των εξυπηρετητών του σχολικού εργαστηρίου από κακόβουλο λογισμικό (spyware / adware) είναι το Spybot Search & Destroy (SpybotSD). Αν και δεν έχει κόστος κτήσης (δίδεται με άδεια freeware) έχει χαρακτηριστικά που συναντώνται σε ανταγωνιστικά εμπορικά προγράμματα.

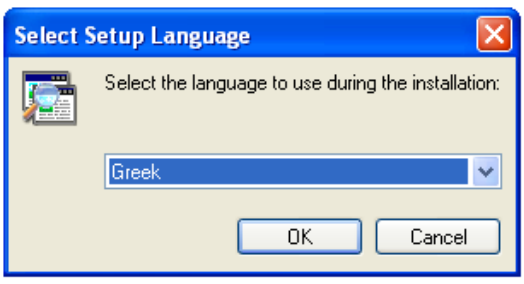
Ανάμεσα στα αξιοσημείωτα χαρακτηριστικά του είναι:

- Η λήψη αντιγράφου ασφαλείας του μητρώου του λειτουργικού συστήματος (windows registry) που μπορεί να χρησιμοποιηθεί για αποκατάστασή του αν για κάποιο λόγο καταστραφεί.
- Η διαδικασία ανοσοποίησης (immunization), εφαρμόζοντας ρυθμίσεις στο λειτουργικό σύστημα και στις εφαρμογές που επικοινωνούν στο Διαδίκτυο (π.χ. Internet Explorer), αποτρέπει την εγκατάσταση κακόβουλου λογισμικού ή απλά αποκλείει την πρόσβαση σε κακόβουλους ιστοχώρους εξ' ολοκλήρου.

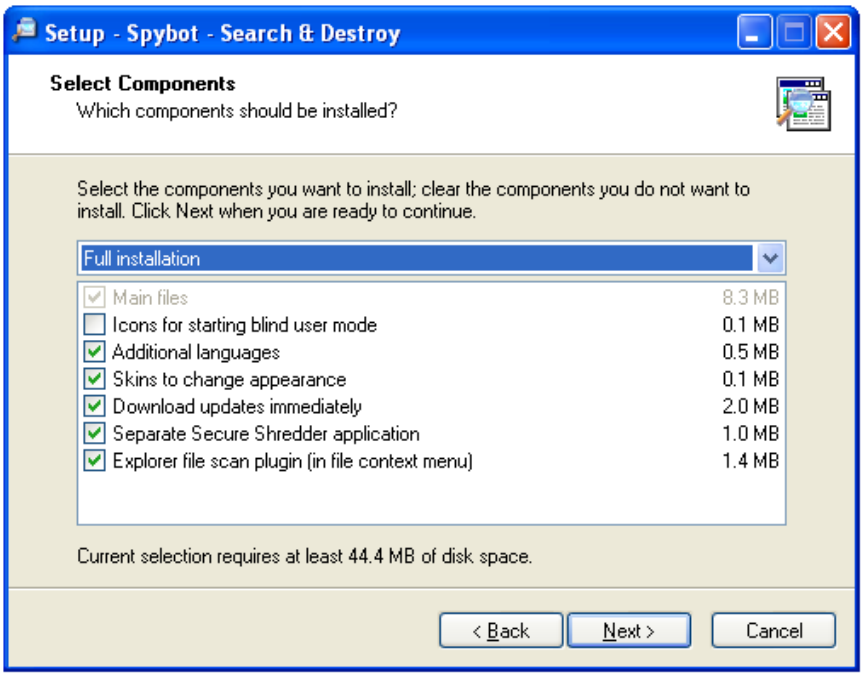
Στις επόμενες παραγράφους περιγράφεται η διαδικασία εγκατάστασης, οι συνηθέστερες λειτουργίες του προγράμματος καθώς και οι δυνατότητες αυτοματοποίησης εκτέλεσης του προγράμματος με χρήση ειδικών επιλογών που δίνονται από την γραμμή εντολών.

1.1 Εγκατάσταση Spybot Search & Destroy

Η εγκατάσταση υποστηρίζει πολλές γλώσσες. Επιλέγοντας είτε Αγγλικά είτε Ελληνικά, από το πρώτο παράθυρο διαλόγου, εμφανίζονται οι επιλογές για τα διάφορα συστατικά στοιχεία που απαρτίζουν το πρόγραμμα.

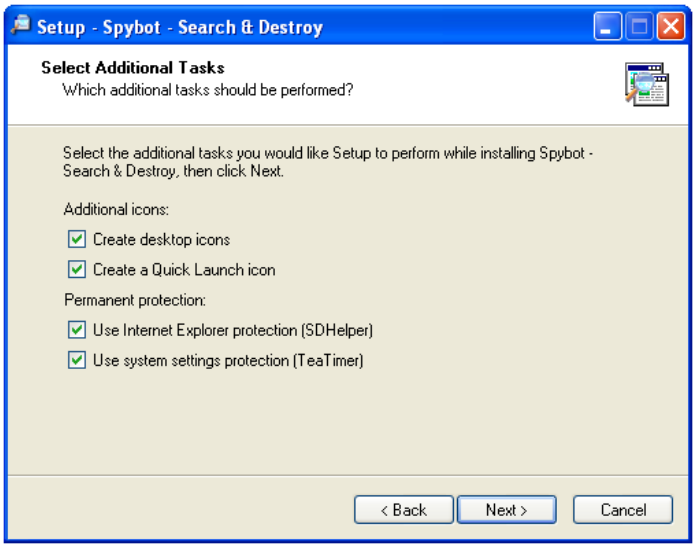


Εικόνα 1 SpybotSD: Εγκατάσταση- Επιλογή γλώσσας



Εικόνα 2 SpybotSD: Εγκατάσταση- Επιλογή συστατικών στοιχείων

Σημείωση: Στις τελευταίες εκδόσεις του προγράμματος υπάρχει δυνατότητα να γίνεται ενημέρωση της λίστας με τα αποτυπώματα κακόβουλου λογισμικού (definitions update) ακόμα και κατά την διάρκεια της εγκατάστασης. Η ενημέρωση συνιστάται να γίνεται πριν από κάθε έλεγχο του λειτουργικού συστήματος (τουλάχιστον μια φορά την εβδομάδα).

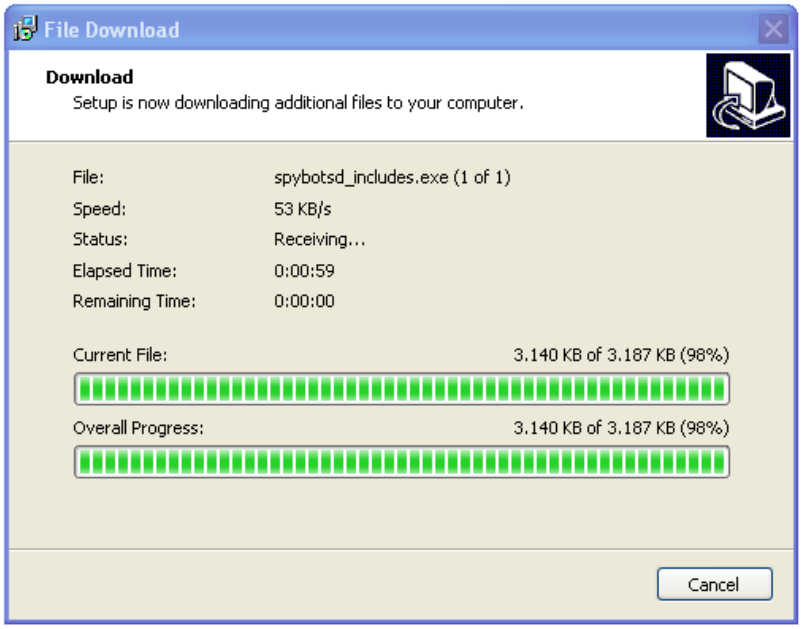


Εικόνα 3 SpybotSD: Εγκατάσταση – Επιπλέον επιλογές

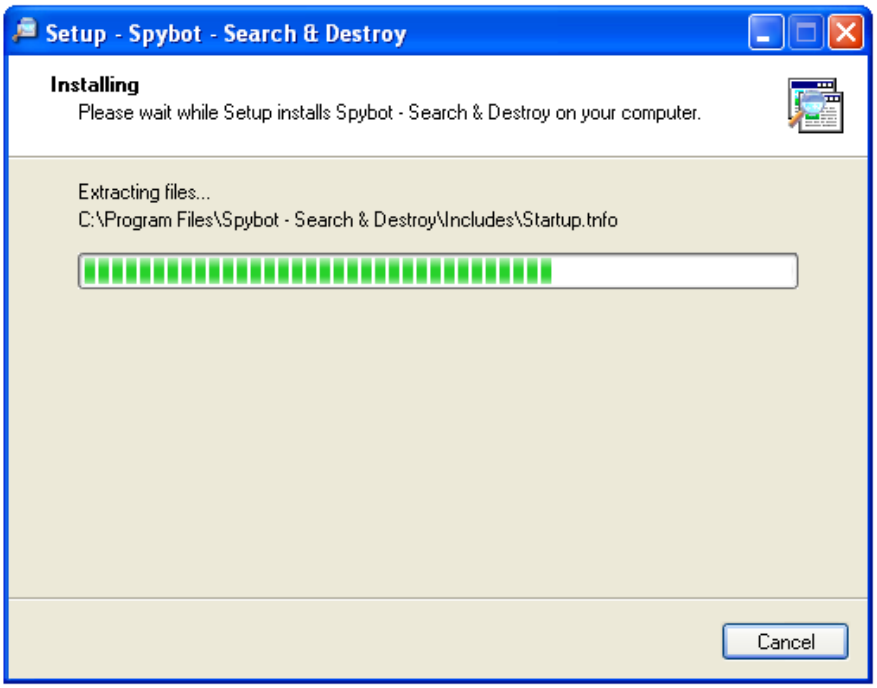
ΠΡΟΣΟΧΗ: Προτείνεται να μείνουν ενεργοποιημένες τις παρακάτω επιλογές:

- Use Internet Explorer protection (SDHelpder) - εφαρμογή που βοηθά τον Internet Explorer εμποδίζοντας την λήψη και εκτέλεση αρχείων από κακόβουλες ιστοσελίδες.
- Use system settings protection (TeaTimer) - εφαρμογή που τρέχει συνεχώς στο παρασκήνιο παρακολουθώντας τις διεργασίες που προσπαθούν να τροποποιήσουν ρυθμίσεις του συστήματος,

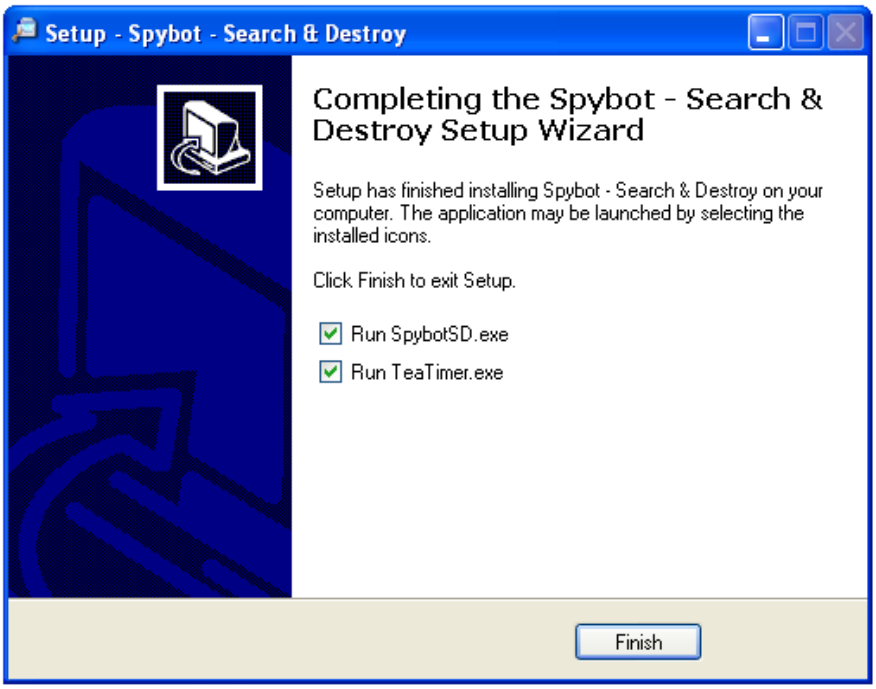
εκτός αν ήδη χρησιμοποιείται το Lavasoft Ad-Aware® SE Professional ή άλλα παρόμοια χαρακτηριστικά σε άλλα προγράμματα προστασίας από spyware, διαφορετικά, μπορεί να εμφανίζονται διπλά μηνύματα.



Εικόνα 4 SpybotSD: Εγκατάσταση – Ενημέρωση εκδόσεων



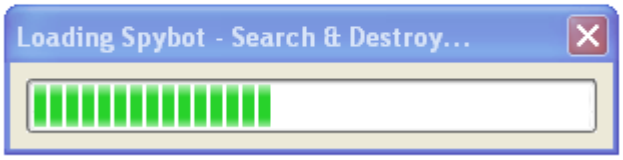
Εικόνα 5 SpybotSD: Εγκατάσταση – Εμφάνιση προόδου



Εικόνα 6 SpybotSD: Εγκατάσταση – Ολοκλήρωση

1.2 Πρώτη εκτέλεση προγράμματος Spybot Search & Destroy

Το πρόγραμμα εκτελείται από το εικονίδιο  οπότε και εμφανίζεται η μπάρα προόδου και η ειδοποίηση για την πιθανότητα δυσλειτουργίας ή και πλήρους απενεργοποίησης εφαρμογών εφόσον αφαιρεθούν τα διαφημιστικά μηνύματα (advertisement robots). Αυτή η πιθανότητα αναφέρεται ρητά στους όρους της άδειας χρήσης της εκάστοτε εφαρμογής (license agreement).

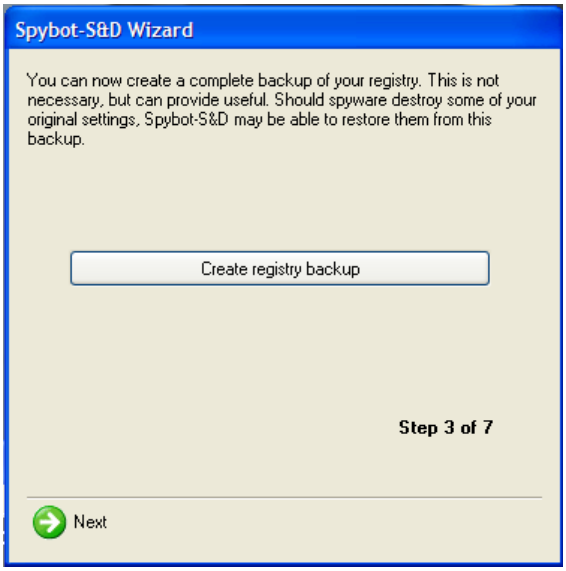


Σημείωση: Αν στις επιλογές της εγκατάστασης είχε επιλεγεί **Run SpybotSD** δεν απαιτείται να χρησιμοποιηθεί το παραπάνω εικονίδιο, αφού, η εφαρμογή θα εκτελεστεί αυτόματα.

Την πρώτη φορά που εκτελείται το πρόγραμμα εμφανίζεται ένας οδηγός με διάφορες εργασίες που προτείνεται να εκτελεσθούν:

1.2.1 Δημιουργία αντιγράφου του μητρώου του λειτουργικού συστήματος (windows registry).

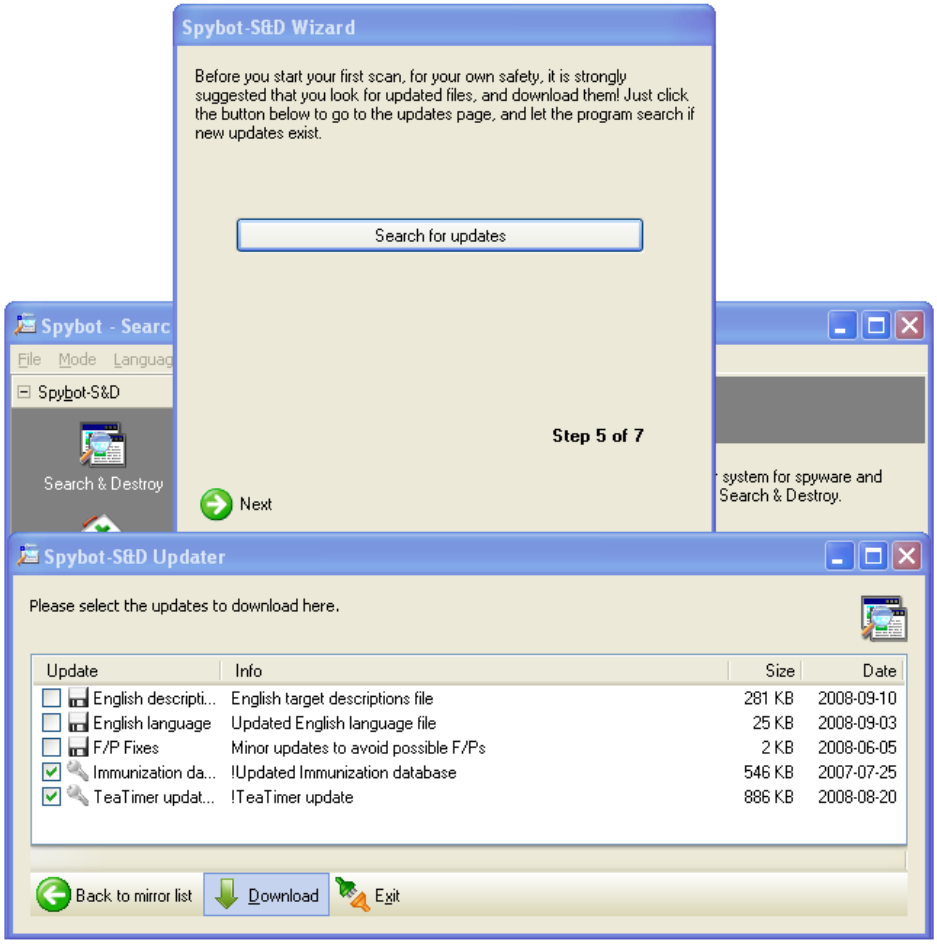
Η δημιουργία του αντιγράφου δεν είναι απαραίτητη αλλά διευκολύνει την επαναφορά των αρχικών ρυθμίσεων αν συμβεί κάποιο σφάλμα. Ένα αντίγραφο του μητρώου δημιουργείται επιλέγοντας το πλήκτρο **Create registry backup**. Μπορεί να περάσουν μερικά λεπτά μέχρι την ενεργοποίηση του πλήκτρου **Next**.



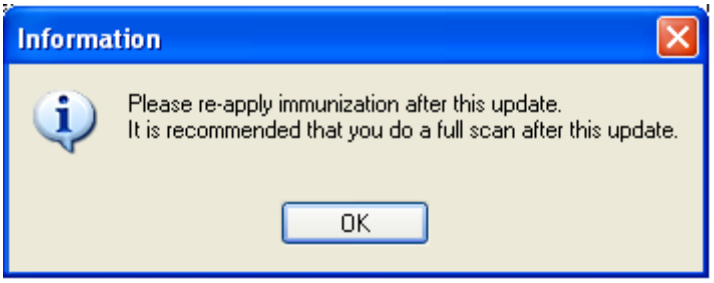
Εικόνα 7 – SpybotSD: Εκτέλεση - Αρχικός οδηγός - Registry Backup

1.2.2 Έλεγχος νέας ενημερωμένης έκδοσης αρχείων.

Επιλέγοντας το πλήκτρο **Search for Updates** το πρόγραμμα συνδέεται στο Διαδίκτυο και ελέγχει για νέες ενημερώσεις (definitions update). Καλή πρακτική είναι ο έλεγχος για νέες εκδόσεις πριν από κάθε ανίχνευση του συστήματος για spyware. Αν βρεθούν νέες ενημερώσεις, εμφανίζεται το πλήκτρο **Download** και μετά επιλέγουμε Next. Αν δεν εντοπισθούν νέες ενημερώσεις επιλέγουμε Next.



Εικόνα 8 – SpybotSD: Εκτέλεση - Αρχικός οδηγός – Search for Updates



Εικόνα 9 – SpybotSD: Εκτέλεση - Αρχικός οδηγός – Immunize prompt

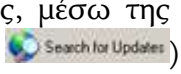
Όταν ολοκληρωθεί η εγκατάσταση των νέων ενημερώσεων και επιλεχθεί **EXIT,** εμφανίζεται ένα ενημερωτικό παράθυρο διαλόγου που αναφέρει συμβουλές και καλές πρακτικές, (να γίνεται πάντα ανοσοποίηση και έλεγχος των αρχείων για spyware μετά από εγκατάσταση νέων αρχείων με αποτυπώματα spyware).

Εάν δεν προταθεί να ανοσοποιηθεί το σύστημα (**Immunize this system**) ή απλά επιλεχθεί να μην γίνει, μπορεί ανά πάσα στιγμή να γίνει ανοσοποίηση από το μενού του κεντρικού προγράμματος.

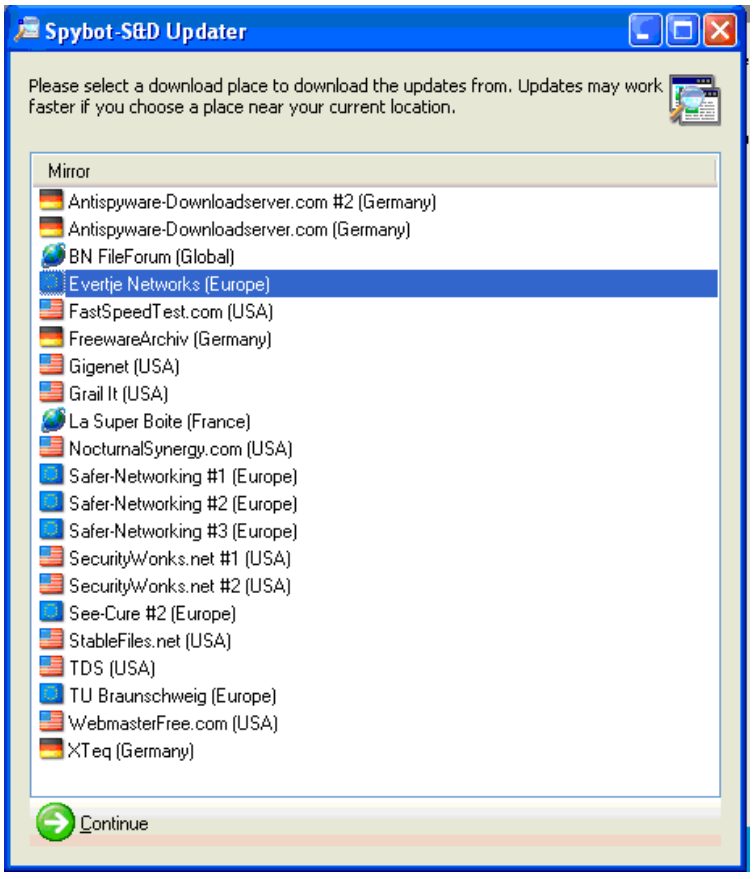
1.3 Χρησιμοποιώντας το Spybot Search & Destroy

1.3.1 Ελέγχοντας το σύστημα

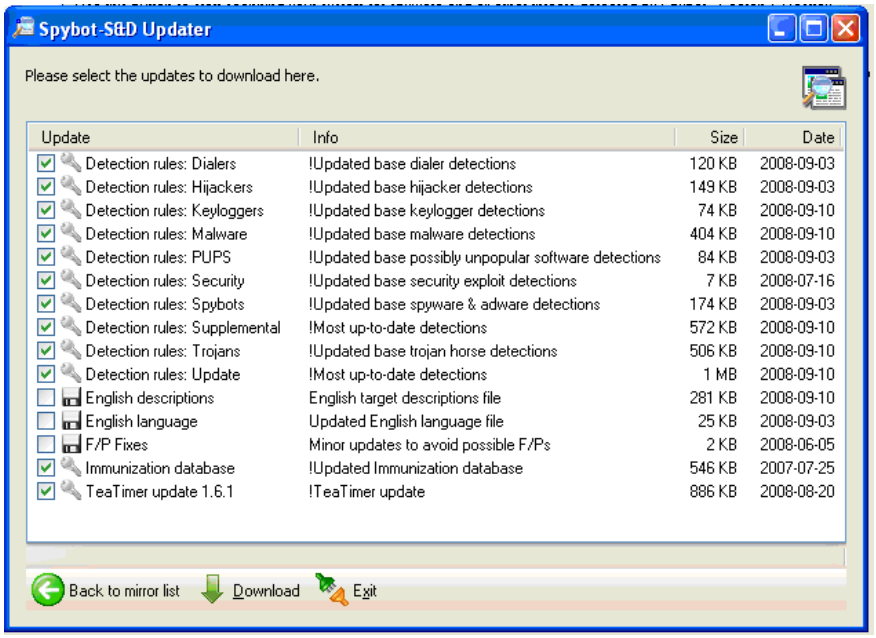
Πάντα πριν την διενέργεια ενός ελέγχου του συστήματος πρέπει να γίνεται έλεγχος για νέες ενημερώσεις, μέσω της επιλογής **Update (εικονίδιο** 

) και **Search For Updates** (εικονίδιο 

). Στο παράθυρο διαλόγου επιλέγεται ο τόπος όπου βρίσκεται ο κοντινότερος εξυπηρετητής αναβάθμισης.

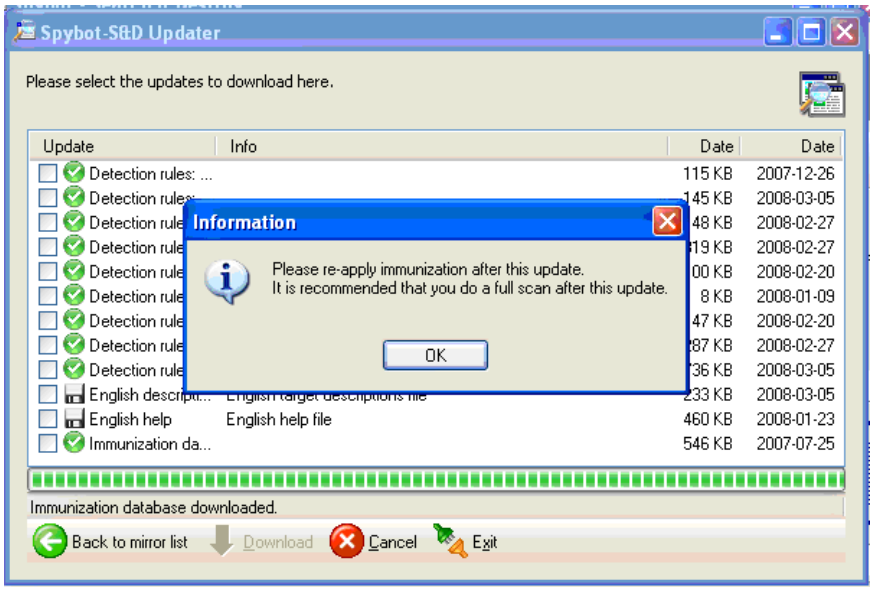


Αφού επιλεχθούν οι αναβαθμίσεις που χρειάζεται να μεταφορτωθούν, στο επόμενο παράθυρο, επιλέγεται το πλήκτρο **Download.**

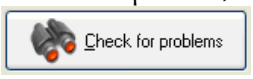


Εικόνα 10 – SpybotSD: Εκτέλεση- Επιλογή επιμέρους Updates

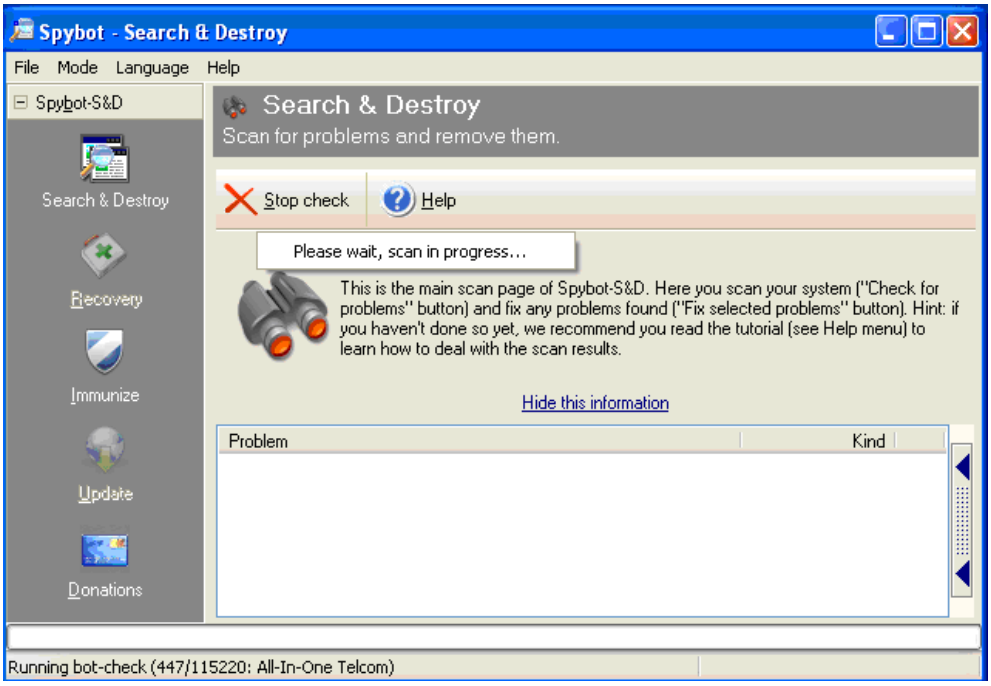
Μετά την ολοκλήρωση των ενημερώσεων, η εφαρμογή προτρέπει στον χρήστη, έχοντας πλέον την τελευταία έκδοση των αποτυπωμάτων των κακόβουλων προγραμμάτων, να γίνει εκ νέου ένας πλήρης έλεγχος του συστήματος (full scan) και νέα ανοσοποίηση (immunization).



Εικόνα 11 – SpybotSD: Εκτέλεση- Ολοκληρώθηκε η ενημέρωση

Έχοντας πλέον την τελευταία έκδοση του προγράμματος και των αποτυπωμάτων, εκτελείται έλεγχος του συστήματος επιλέγοντας το εικονίδιο 

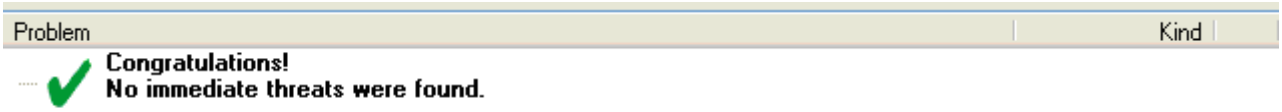
, οπότε και ξεκινά ο έλεγχος των ρυθμίσεων, του μητρώου, και των αρχείων του συστήματος.



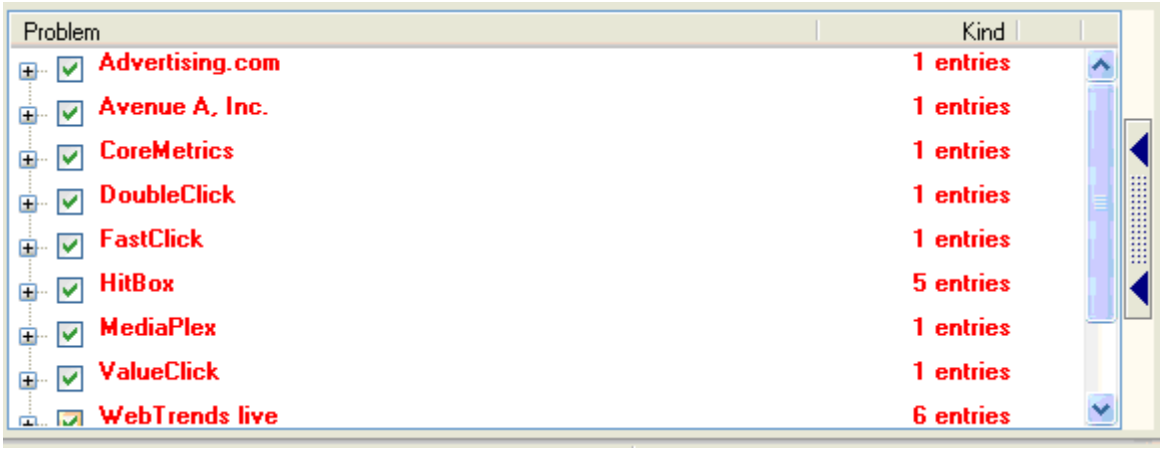
Εικόνα 12 – SpybotSD: Έλεγχος για κακόβουλο λογισμικό

Η πρόοδος του ελέγχου εμφανίζεται σε μια μπάρα στο κάτω μέρος του παραθύρου (την πρώτη φορά μπορεί να διαρκέσει μερικά λεπτά).

Όταν ολοκληρωθεί η αναζήτηση εμφανίζονται τα αποτελέσματα στο πλαίσιο. Σε αυτά υπάρχει ενημέρωση, είτε ότι δεν υπάρχουν προβλήματα είτε ότι υπάρχουν παρέχοντας λεπτομερή αναφορά με το όνομα, τον τύπο και τον αριθμό των προβλημάτων.



Εικόνα 13 – SpybotSD: Έλεγχος για κακόβουλο λογισμικό - Δεν βρέθηκαν προβλήματα



Εικόνα 14 – SpybotSD: Έλεγχος για κακόβουλο λογισμικό - Βρέθηκαν προβλήματα

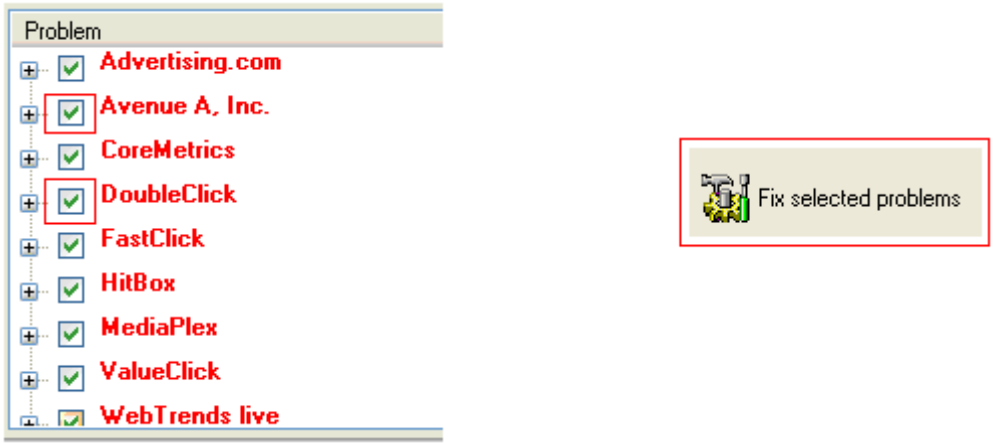
1.3.2 Κατανοώντας τα αποτελέσματα του κακόβουλου λογισμικού

Αφού το spybot έχει ολοκληρώσει τον έλεγχο, τα αποτελέσματα εμφανίζονται κατηγοριοποιημένα. Με κόκκινο χρώμα εμφανίζονται τα προβλήματα spyware που πρέπει να επιδιορθωθούν και με πράσινο χρώμα εμφανίζονται τα ίχνη χρήσης (usage tracks). Τα ίχνη χρήσης δεν είναι απαραίτητο να αφαιρεθούν μιας και δεν αποτελούν άμεσο κίνδυνο για το σταθμό εργασίας αλλά περιέχουν αποθηκευμένες πληροφορίες για παλαιότερες ενέργειες που έχουν εκτελεστεί στο σύστημα.

Κάνοντας κλικ στο πλαίσιο δεξιά μιας απειλής που ανιχνεύθηκε και εμφανίζεται στη λίστα, προβάλλονται περισσότερες πληροφορίες σχετικά με την συγκεκριμένη απειλή. Επίσης, κάθε απειλή έχει και ένα εικονίδιο με ένα σταυρό, που αν επιλεχθεί με το ποντίκι, εμφανίζονται οι ξεχωριστές πληροφορίες για κάθε μια από τις εγγραφές του προβλήματος σε αυτή την κατηγορία.

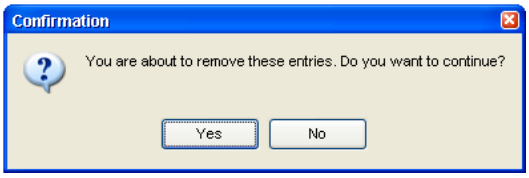
1.3.3 Αφαιρώντας κακόβουλο λογισμικό

Για να αφαιρέσουμε ένα πρόβλημα που βρέθηκε σε προηγούμενο βήμα ελέγχου, επιλέγουμε με το ποντίκι (tick ☑) και πατάμε το κουμπί **Fix Selected Problems**.



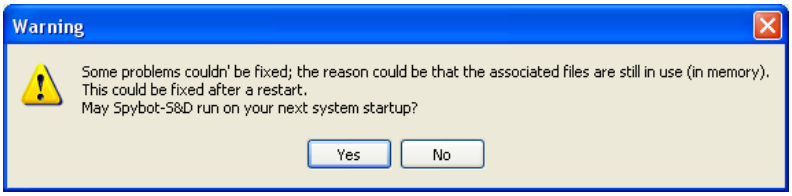
Εικόνα 15 – SpybotSD: Αφαίρεση κακόβουλου λογισμικού - Επιλογή και επιδιόρθωση

Αν εμφανιστεί κάποια προειδοποίηση ότι πρόκειται να αφαιρεθούν τα επιλεγμένα προβλήματα επιλέγεται NAI (yes).



Εικόνα 16 – SpybotSD: Αφαίρεση κακόβουλου λογισμικού - Επιβεβαίωση

Σημείωση: Ορισμένες φορές μπορεί το spybotSD για να ολοκληρώσει την αφαίρεση του κακόβουλου λογισμικού να κάνει επανεκκίνηση του σταθμού εργασίας



Εικόνα 17 – SpybotSD: Αφαίρεση κακόβουλου λογισμικού - Απαιτείται επανεκκίνηση ΗΥ

1.3.4 Ανοσοποίηση

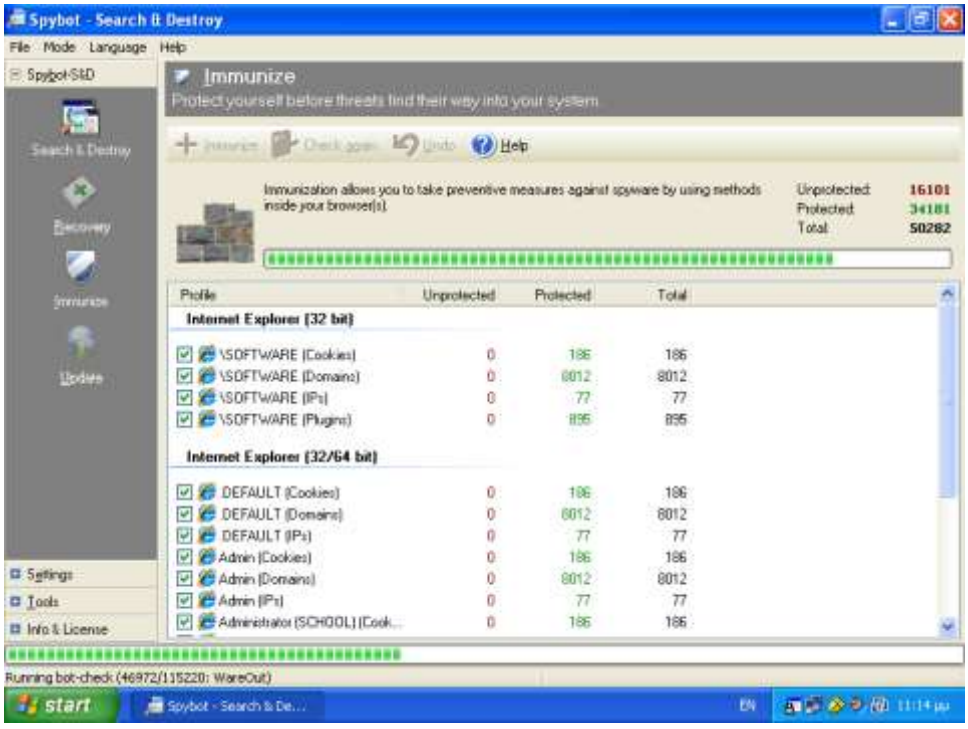
Μια άλλη λειτουργία του spybotSD είναι η ανοσοποίηση (immunization) που βοηθά ώστε να μην εγκαθίστανται λογισμικά spyware στο σύστημα. Αυτό γίνεται κάνοντας ειδικές ρυθμίσεις στα προγράμματα πλοήγησης (Internet Explorer,

Firefox) ώστε να αποφεύγεται η μεταφόρτωση του κακόβουλου λογισμικού και η επικοινωνία με γνωστές κακόβουλες διευθύνσεις IP / ιστοσελίδες.

Η ανοσοποίηση γίνεται επιλέγοντας το πλήκτρο **Immunize**, στο αριστερό μενού, και έπειτα το εικονίδιο

Εικόνα 18 – SpybotSD: Ανοσοποίηση μηχανήματος

Κατά την διάρκεια της ανοσοποίησης εμφανίζεται μια μπάρα προόδου και αριθμητικά οι εγγραφές που επεξεργάσθηκαν.



Εικόνα 19 – SpybotSD: Ανοσοποίηση μηχανήματος – πρόοδος ανοσοποίησης

1.3.5 Επαναφορά συστήματος

Μια άλλη λειτουργία του spybotSD είναι η επαναφορά (recovery) που βοηθά το σύστημα να επανέλθει μετά από επιδιόρθωση προβλημάτων, διατηρώντας ένα

αντίγραφο από όλα τα προβλήματα που έχουν επιδιορθωθεί. Αυτό είναι χρήσιμο αν κάτι σβηστεί κατά λάθος.

Για να επανέλθει μια εγγραφή που είχε επιδιορθωθεί παλαιότερα ακολουθούνται τα παρακάτω βήματα:

1. Επιλέγεται το πλήκτρο επαναφορά (Recovery 

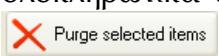
) στο αριστερό μενού οπότε εμφανίζεται μια λίστα με τα προβλήματα που έχουν αποθηκευθεί και επαναφέρονται.

Εικόνα 20 – SpybotSD: Επαναφορά συστήματος

2. Μαρκάρεται με το ποντίκι (tick ) και στη συνέχεια Recover selected items 

.

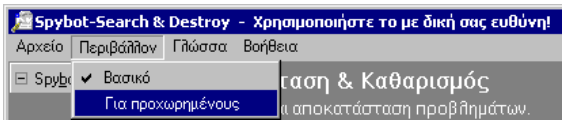
Σημείωση: Τα προβλήματα από spyware πρέπει να επανέρχονται με προσοχή μιας και η ενέργεια αυτή θα οδηγήσει και σε επανεγκατάσταση του spyware λογισμικού στο σύστημα σας.

Αντικείμενα που εμφανίζονται στην λίστα της επαναφοράς δεν αποτελούν απειλή για το σύστημα αλλά, αν είναι επιθυμητό, μπορούν να διαγραφούν ολοκληρωτικά επιλέγοντας τα και πατώντας το κουμπί Purge selected items 

.

1.3.6 Ρυθμίσεις για προχωρημένους

Από το βασικό μενού επιλέγεται η προβολή ρυθμίσεων για προχωρημένους χρήστες, ακολουθώντας την διαδρομή Περιβάλλον -> για προχωρημένους (mode -> advanced mode), οπότε και εμφανίζεται και μια προειδοποίηση



Εικόνα 21 – SpybotSD: Ρυθμίσεις για προχωρημένους

Εικόνα 22 – SpybotSD: Ρυθμίσεις για προχωρημένους - Προειδοποίηση

Από το νέο μενού δίνεται η δυνατότητα αλλαγής της γλώσσας της εφαρμογής καθώς και πολλών από τις ρυθμίσεις που καθορίζουν την συμπεριφορά της. Σημειώνονται επιγραμματικά οι δυνατότητες :

- Αλλαγή της προτεραιότητας εκτέλεσης της εφαρμογής.
- Ενεργοποίηση ή απενεργοποίηση της δημιουργίας αντιγράφων ασφαλείας κατά την επιδιόρθωση προβλημάτων από κακόβουλο λογισμικό / ίχνη χρήσης κλπ.

1.4 Αυτοματοποίηση εκτέλεσης Spybot Search & Destroy

Για να εκτελεστεί το πρόγραμμα είτε χρησιμοποιείται η διεπιφάνεια χρήστη είτε οι διακόπτες / παράμετροι που δίδονται στο εκτελέσιμο αρχείο από τη γραμμή εντολών (command prompt). Οι εντολές που το εκτελέσιμο Spybot-S&D (SpybotSD.exe) μπορεί αναγνωρίζει είναι:

- **/taskbarhide**
  Εκτελείται το Spybot-S&D κρυμμένο από τον τελικό χρήστη (χωρίς να εμφανίζεται παράθυρο, ή εικονίδιο στην γραμμή εργαλείων). Θα πρέπει πάντα να χρησιμοποιείται σε συνδυασμό με την εντολή **/autoclose** (διαφορετικά θα παραμείνει ενεργό δεσμεύοντας άσκοπα πόρους του υπολογιστή). Η εντολή αυτή είναι χρήσιμη μόνο σε συνδυασμό με τις επιλογές **/autocheck**, **/autoupdate** ή **/autoimmunize** διότι μόνο με αυτές μπορεί ο χρήστης να δώσει απευθείας εντολές στο πρόγραμμα που εκτελείται κρυμμένο.
- **/minimized**
  Εκτελείται η εφαρμογή σε ελαχιστοποιημένο παράθυρο.
- **/uninstall** (απαρχαιομένη)
  Χρησιμοποιούνταν σε παλιότερες εκδόσεις για την απεγκατάσταση της εφαρμογής Spybot-S&D. Αυτή η εντολή δεν πρέπει να χρησιμοποιείται πλέον, αφού υπάρχει εκτελέσιμο αρχείο - unins000.exe για αυτή την λειτουργία.
- **/blinduser**
  Η εφαρμογή εμφανίζει ειδικά μενού για χρήστες με περιορισμένη ή καθόλου όραση.
- **/allhives**
  Η εφαρμογή ελέγχει όλα τα εγκατεστημένα λειτουργικά συστήματα windows στο σκληρό δίσκο, τις ανενεργές εγκαταστάσεις ακόμα και τα περιεχόμενα του registry. Περισσότερες πληροφορίες βρίσκονται στις συχνές ερωταποκρίσεις http://www.safer-networking.org/en/faq/41.html).
- **/autoupdate**
  Η εφαρμογή προσπαθεί να κάνει ενημέρωση του προγράμματος μόλις εκκινήσει.
- **/autocheck**
  Η εφαρμογή ελέγχει αρχεία μόλις εκκινήσει.
- **/autofix**
  Η εφαρμογή επιδιορθώνει αμέσως όποιο πρόβλημα εντοπίζεται.

- **/autoclose**
  Η εφαρμογή κλείνει όταν ολοκληρωθεί η εργασία που ζητήθηκε να εκτελεστεί (είτε είναι ενημέρωση, είτε έλεγχος αρχείων).
- **/autoimmunize**
  Η εφαρμογή εκτελεί την διαδικασία ανοσοποίησης αρχείων.
- **/onlyspyware**
  Η εφαρμογή επιδιορθώνει μόνο τα προβλήματα που οφείλονται σε spyware (κόκκινο χρώμα) με την επιλογή **/autofix**, χωρίς να τροποποιεί τα ίχνη χρήσης των προγραμμάτων.
- **/easymode**
  Η εφαρμογή εμφανίζει πιο εύκολη στην χρήση διεπαφή (Interface).
- **/createenglish**
  Αυτή η επιλογή ενημερώνει το αρχείο English.sbl με τα τελευταία κείμενα, και είναι χρήσιμη μόνο σε χρήστες που κάνουν μετάφραση σε άλλες γλώσσες.

Σημείωση: Πρέπει να δοθεί προσοχή στην διαδρομή που βρίσκεται το εκτελέσιμο Spybot-S&D καθώς πρέπει να περιέχεται μέσα σε εισαγωγικά και οι πολλαπλές παράμετροι πρέπει να χωρίζονται με κενά.

Παράδειγμα αυτοματοποίησης της ενημέρωσης και διενέργειας ελέγχου/ επιδιόρθωσης από το πρόγραμμα:

"C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /taskbarhide /autoclose /autocheck /autofix /onlyspywar

Υπάρχει η δυνατότητα να αυτοματοποιηθεί η εκτέλεση των παραπάνω ενεργειών αν δημιουργηθεί ένα αρχείο δέσμης εντολών (.bat ή .cmd file). Συνιστάται να εκτελείται αυτόματα το spybot μέσω των “scheduled tasks” των Windows.

Περισσότερες πληροφορίες για τη δημιουργία ενός scheduled task σε γραμμή εντολών υπάρχουν στην παρακάτω ιστοσελίδα της Microsoft http://support.microsoft.com/kb/814596/en-us.

Οι παραπάνω οδηγίες συντάχθηκαν με τη συνεργασία του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης/Κέντρο Λειτουργίας Δικτύου (ΑΠΘ/ΚΛΔ, www.auth.gr , noc.auth.gr).