

Πίσω από τα τείχη

Τον κλασικό προβληματισμό «μα καλά, με εμένα θα ασχοληθούν;» καλό είναι να τον αποβάλλουμε το συντομότερο δυνατόν. Βλέπετε, οι επιθέσεις μπορεί να μην αφορούν σε εμάς συγκεκριμένα, είναι όμως τυχαίες, τυφλές και μαζικές!

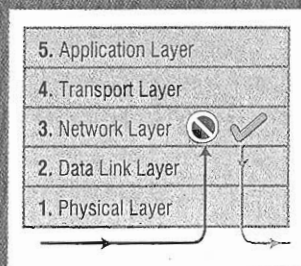
ΑΡΚΕΙ ΠΟΥ Ο ΥΠΟΛΟΓΙΣΤΗΣ ΜΑΣ είναι συνδεδεμένος στο Διαδίκτυο. Αυτοματοποιημένα προγράμματα σαρώνουν το Internet προκειμένου να ανακαλύψουν υπολογιστές με γνωστές «τρύπες» ασφαλείας και να τραβήξουν μέσα από αυτές—πάλι αυτά—τα όποια πολύτιμα προσωπικά δεδομένα, όπως, π.χ., κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών, που φυλάμε στον υπολογιστή μας. Πέραν τούτου, ο υπολογιστής μπορεί να γίνει ερμήν μας το ορμητήριο ενός cracker, που μας «φύτεψε» ύπουλα ένα κακόβουλο προγραμματάκι, όπως και σε χιλιάδες άλλους ευάλωτους υπολογιστές ανά τον κόσμο. Ξαφνικά, μια προγραμματισμένη από τον cracker μέρα και ώρα, το PC μας, μαζί με όλα τα άλλα που έχουν παραβιαστεί, θα εξαπολύσει μια σιωπηλή επιδρομή σε κάποιον Web server ζητώντας όλοι να δούνε—πάντα σιωπηλά—τις σελίδες του. Ο server δεν θα μπορέσει να ανταπεξέλθει σε τόσα πολλά αιτήματα ταυτόχρονα και θα καταρρεύσει. Χωρίς καν να το ξέρουμε, και μάλλον χωρίς ποτέ να το μάθουμε, λάβαμε μέρος σε μια επίθεση DDoS (Distributed Denial of Service). Θα επιτρέψουμε να συμβούν σε εμάς όλα αυτά; Όχι, βέβαια! Ας πάρουμε την κατάσταση στα χέρια μας, τώρα!

ΑΡΧΕΣ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ. Για να προστατευτούμε όσο το δυνατόν αποτελεσματικότερα από τις όποιες διαδικτυακές επιβουλές, οφείλουμε πρώτα να γίνουμε καλοί γνώστες των θεμελιωδών αρχών που διέπουν την επικοινωνία σε αυτό. Όπως και να το κάνουμε, δεν είναι δυνατόν να θέλουμε να ασχοληθούμε σοβαρά με τη ρύθμιση ενός firewall και ταυτόχρονα να μη γνωρίζουμε μερικούς βασικούς όρους, όπως διεύθυνση IP, θύρα (port), πρωτόκολλο επικοινωνίας (HTTP, FTP, SMTP κ.ά.), καθώς και πρωτόκολλο μεταφοράς (TCP, UDP,

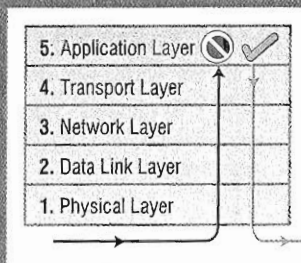
ICMP κ.ά.). Αυτοί οι τέσσερις όροι είναι το A και το Ω στις δικτυακές επικοινωνίες και η κατανόησή τους αποτελεί ένα από τα πλέον απαραίτητα ορμητικά όπλα.

• **Διεύθυνση IP (IP address).** Η διεύθυνση IP αποτελεί τη βασική μας ταυτότητα στο Internet. Μας δίνεται από τον ιντερνετικό μας φορέα (Internet Service Provider ή ISP) κάθε φορά που συνδεόμαστε στο Internet. Βάσει αυτής είναι δυνατό ο εντοπισμός και η σύναψη επικοινωνίας με οποιονδήποτε υπολογιστή στο Διαδίκτυο (ο οποίος φυσικά θα φέρει τη δική του, μοναδική διεύθυνση IP). Αν θέλετε αυτή τη στιγμή να δείτε τη διεύθυνση IP του υπολογιστή σας (για την ακρίβεια την IP της δικτυακής συσκευής σας, όπως είναι το μόντεμ ή η κάρτα δικτύου), ανοίξτε μια κονσόλα γραμμής εντολών (π.χ., <Start>Run>cmd>) και πληκτρολογήστε ipconfig (winipcfg για λειτουργικά Windows 9x/Me).

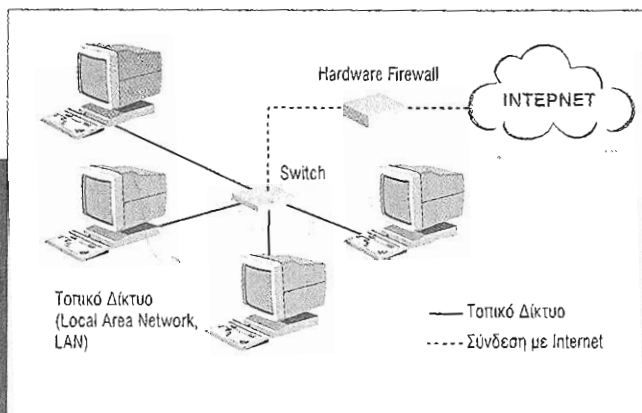
• **Θύρες επικοινωνίας (ports).** Εκτός από το IP, που είναι μοναδικό



Στο τρίτο επίπεδο της στοίβας TCP/IP μπορούν να ελεγχθούν οι διευθύνσεις παραλήπτη και αποστολέα, οι χρησιμοποιούμενες θύρες επικοινωνίας και το πρωτόκολλο μεταφοράς (π.χ., TCP, UDP). Αυτό είναι το επίπεδο στο οποίο λειτουργούν τα hardware firewall.



Το πέμπτο επίπεδο είναι αυτό που βασύως στο μικροκόσμιο τα personal firewall. Εδώ μπορούν να υλοποιηθούν κανόνες που εμπλέκουν τα πρωτόκολλα των εφαρμογών (HTTP, IRC, FTP κ.ά.). Επίσης, είναι δυνατός και ο έλεγχος των περιεχομένων των διακινούμενων πακέτων.



Το firewall προστατεύει έναν υπολογιστή ή ένα δίκτυο υπολογιστών από επιθέσεις ή «αδιάκριτες» ενέργειες, που εκπορεύονται από μηχανήματα κάποιου άλλου δικτύου—συνήθως του Internet. Τα firewall ενδέχεται να είναι είτε συσκευές υλικού (hardware firewall), προστατεύοντας έναν μόνο ή περισσότερους υπολογιστές, είτε λογισμικό (personal firewall) προστατεύοντας τον υπολογιστή στον οποίο είναι εγκατεστημένο. Η ουσιαστική λειτουργία του firewall είναι να υποβάλλει τα εισερχόμενα και εξερχόμενα δεδομένα σε μια σειρά από ελέγχους και να τα αφήνει να διέλθουν ή να τα εμποδίζει, ανάλογα με το αν περνούν τα τεστ ή όχι.

κό για κάθε υπολογιστή, υπάρχουν οι θύρες επικοινωνίας (ports) που διατηρεί ανοιχτές ή κλειστές ο υπολογιστής (ακριβέστερα, το λειτουργικό σύστημα που γνωρίζει το πρωτόκολλο TCP/IP). Αυτές χρησιμοποιούνται για τον εξής λόγο: Σε κάθε υπολογιστή μπορεί να «τρέχουν» παράλληλα πολλά προγράμματα που σχετίζονται με ένα άλλο δίκτυο, όπως είναι το Internet. Για να είναι ομαλή η επικοινωνία τους με τον «έξω κόσμο», κάθε πρόγραμμα κάνει χρήση συγκεκριμένων θυρών, μέσω των οποίων «μιλάει» με τους υπόλοιπους υπολογιστές του Internet. Έτσι, όποτε φτάνει στο μηχανήμα μας η απάντηση μιας αίτησης για την προβολή κάποιας ιστοσελίδας, ο browser την «αντιλαμβάνεται» μέσω της κατάλληλης θύρας και κατόπιν δέχεται, στην ίδια θύρα, τα δεδομένα της ίδιας της σελίδας. Την ίδια στιγμή, από μία άλλη θύρα ένα πρόγραμμα FTP μπορεί να κατεβάζει ένα αρχείο, από κάποια άλλη θύρα επικοινωνεί το αγαπημένο μας πρόγραμμα Instant Messaging κ.ο.κ. Κάθε θύρα ταυτοποιείται από έναν αριθμό μήκους 16bit, επομένως υπάρχουν 2^{16} , δηλαδή 65.535 διαφορετικές θύρες.

- **Πρωτόκολλα επικοινωνίας (communication protocols).** Αφού πραγματοποιηθεί η σύνδεση μεταξύ δύο προγραμμάτων δύο διαφορετικών υπολογιστών, πάντα μέσω των θυρών που χρησιμοποιούν τα αντίστοιχα προγράμματα, η επικοινωνία επιτυγχάνεται ακολουθώντας ένα συγκεκριμένο πρωτόκολλο. Αυτό δεν είναι τίποτε άλλο από ένα σύνολο προδιαγραφών και εντολών, μια συγκεκριμένη «γλώσσα», θα λέγαμε, κατανοητή και από τα δύο μέρη της σύνδεσης. Δημοφιλές παράδειγμα πρωτοκόλλου επικοινωνίας είναι το HTTP, για την περιήγηση στον Παγκόσμιο Ιστό.

- **Πρωτόκολλα μεταφοράς (transport protocols).** Για τη διακίνηση των πακέτων απαιτείται ένας μηχανισμός που είναι επιφορτισμένος με την παρακολούθηση της σύνδεσης, ώστε να βεβαιωθεί ότι το πακέτο πράγματι έφτασε στον προορισμό του, να το ξαναστέλνει αν για κάποιο λόγο απέτυχε η αποστολή κ.ο.κ. Το ρόλο αυτό τον επιτελούν τα πρωτόκολλα μεταφοράς. Δημοφιλέστατο παράδειγμα πρωτοκόλλου μεταφοράς αποτελεί το Transmission Control Protocol (TCP), που χρησιμοποιείται στο Internet.

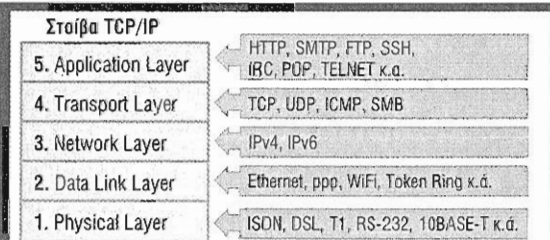
Συνοψίζοντας τα παραπάνω, παραθέτουμε ένα καθημερινό παράδειγμα. Έστω ότι θέλουμε να επισκεφθούμε τον τόπο <http://www.in.gr> Πληκτρολογώντας τη διεύθυνσή του στην μπάρα διευθύνσεων του browser της προτίμησής μας, συμβαίνουν τα εξής: α. Με τη βοήθεια του συστήματος DNS, η ονομαστική διεύθυνση www.in.gr μεταφράζεται στην αριθμητική διεύθυνση IP, εν προκειμένω στην 194.63.247.208. β. Ο browser πραγματοποιεί σύνδεση, μέσω της θύρας 80, με τον απομακρυσμένο διακομιστή. γ. Ο υπολογιστής μας «μιλάει» με τον απομακρυσμένο δια-

κομιστή Service Pack 2 των Windows XP προσφέρει, μεταξύ άλλων, ένα βελτιωμένο, σε σύγκριση με το παλιό, personal firewall. Για να το ενεργοποιήσουμε πηγαίνουμε στο «Control Panel», επιλέγουμε «Network Connections» και με δεξί κλικ στη σύνδεση που μας ενδιαφέρει διαλέγουμε «Properties». Από την ταμπέλα «Advanced» επιλέγουμε «Settings» (στα Windows XP χωρίς SP2 τσεκάρουμε απλώς το κουτάκι «Protect my computer and network by limiting or...») και θέτουμε το firewall σε κατάσταση «On». Από τις ταμπέλες «Exceptions» και «Advanced» μπορούμε να προβάμε σε λεπτομερέστερες ρυθμίσεις. Ενώ όμως το firewall των Windows προσφέρει ικανοποιητική προστασία και έλεγχο της εισερχόμενης κίνησης, δεν παρέχει καμία απολύτως μορφή προστασίας για την εξερχόμενη! Έτσι, σε ένα σενάριο όπου, π.χ., κάποιο trojan επιχειρεί να στείλει «εκεί έξω» ευαίσθητα προσωπικά μας δεδομένα, το firewall των Windows XP δεν θα κάνει τίποτε απολύτως! Για να μη μακρηγορούμε, αν η ασφάλεια σας ενδιαφέρει πραγματικά, απενεργοποιήστε το και στραφείτε στις αποτελεσματικότερες υλοποιήσεις τρίτων κατασκευαστών, αρκετές από τις οποίες διατίθενται και δωρεάν (βλ., π.χ., ZoneAlarm και Kerio Personal Firewall).

κομιστή χρησιμοποιώντας το πρωτόκολλο HTTP, ενώ την ίδια στιγμή το πρωτόκολλο επικοινωνίας TCP φροντίζει για τη διακίνηση των πακέτων πληροφορίας. Πρόγευση για όσα ακολουθούν: Τα απολύτως βασικά πράγματα που μπορεί να ελέγξει κάθε firewall έχουν να κάνουν με τις διευθύνσεις IP, τις θύρες και τα πρωτόκολλα μεταφοράς.

ΘΕΜΕΛΙΩΔΗΣ ΛΙΘΟΣ ΠΛΗΡΟΦΟΡΙΑΣ. Όταν δύο υπολογιστές επικοινωνούν μεταξύ τους με τον τρόπο που αναφέραμε προηγουμένως, αυτό που κάνουν ουσιαστικά είναι να ανταλλάσσουν πακέτα πληροφορίας. Για την ακρίβεια, κάθε πακέτο φέρει μέρος της διακινούμενης πληροφορίας. Σε ένα οποιοδήποτε πακέτο διακρίνουμε δύο βασικά μέρη: την κεφαλίδα (header) και την περιοχή δεδομένων (data ή payload). Η κεφαλίδα, μεταξύ άλλων, περιλαμβάνει τρία πολύ σημαντικά στοιχεία: τις διευθύνσεις IP αποστολέα και παραλήπτη, τις εμπλεκόμενες θύρες επικοινωνίας, καθώς και το πρωτόκολλο που λαμβάνει μέρος στη μεταφορά του πακέτου (TCP, UDP, ICMP κ.ά.). Η βασική λειτουργία των firewall στηρίζεται σε αυτά ακριβώς τα στοιχεία. Όταν ένα πακέτο προσπαθεί να εισέλθει ή να εξέλθει από τον υπολογιστή μας, η κεφαλίδα είναι το βασικό στοιχείο που υπόκειται στο «βάσανο» των κανόνων του firewall. Εάν περάσει από όλες τις δοκιμασίες, τότε και μόνο τότε συνεχίζει το ταξίδι του.

ΔΙΚΤΥΩΣΗ TCP/IP. Η αρχιτεκτονική της λεγόμενης στοιβάς του ζεύγους πρωτοκόλλων TCP/IP (TCP/IP stack), πάνω στην οποία



Η αρχιτεκτονική πάνω στην οποία στηρίζεται η δικτύωση διαφορετικών υπολογιστών, ανεξάρτητα από το λειτουργικό σύστημα ή το φυσικό μέσο μετάδοσης κ.λπ., αποτελείται από πέντε επίπεδα. Όταν έρχονται δεδομένα στον υπολογιστή μας, ακολουθείται η διαδρομή από κάτω προς τα πάνω, ενώ, όταν φεύγουν προς τον «έξω» κόσμο, ακολουθείται η αντίστροφη πορεία. Κάθε επίπεδο είναι επιφορτισμένο με συγκεκριμένους ρόλους, τους οποίους καθορίζει το εκάστοτε πρωτόκολλο που χρησιμοποιείται.

«πατάει» όλη η φιλοσοφία του Διαδικτύου (ανεξαρτήτως λειτουργικού συστήματος, ενσύρματου ή ασύρματου τρόπου μετάδοσης κ.ο.κ.), αποτελείται από πέντε συγκεκριμένα επίπεδα [layers]. Η γνώση του ρόλου ορισμένων από αυτά συμβάλλει στην κατανόηση της λειτουργίας των firewall και ταυτόχρονα στην αποτελεσματικότερη ρύθμισή τους. Το πρώτο επίπεδο (Physical Layer) της στοιβας (στο κάτω μέρος της) αφορά κυρίως στο φυσικό μέσο μετάδοσης και στις τεχνικές που χρησιμοποιούνται ώστε να επιτευχθεί η τελευταία. Το επόμενο επίπεδο (Data Link Layer) ορίζει τις διαδικασίες που απαιτούνται για τη μεταφορά των δεδομένων και εξασφαλίζει ότι αυτά φτάνουν στον προορισμό τους. Μεταξύ των πρωτοκόλλων που χρησιμοποιούνται για το σκοπό αυτό είναι το πολύ γνωστό Ethernet (στις κάρτες δικτύου) και το PPP (στις συνδέσεις dial-up). Από το τρίτο επίπεδο (Network Layer) και μετά αρχίζει το ενεργό παιχνίδι των firewall, αφού πλέον έχουμε επαφή με αναγνωρίσιμο και συνεπώς ελέγξιμο δεδομένα. Το Network Layer είναι υπεύθυνο για τη δημιουργία και τη δρομολόγηση των δικτυακών πακέτων, γεγονός που μεταξύ άλλων σημαίνει ότι είναι υπεύθυνο για τα περιεχόμενα των κεφαλίδων. Προφανώς, κάπου εδώ μπορεί να εμπελαστεί ένα firewall, ελέγχοντας τις διευθύνσεις αποστολέα και παραλήπτη, όπως επίσης τις θύρες και το πρωτόκολλο μεταφοράς (π.χ., TCP, UDP) μιας συγκεκριμένης συνεδρίας (session). Να τονιστεί ότι σε αυτό το επίπεδο δεν μπορεί να γίνει κανένας απολύτως έλεγχος στα δεδομένα (payload) που φέρουν τα πακέτα. Το τέταρτο επίπεδο (Transport Layer) αφορά στα πρωτόκολλα που είναι υπεύθυνα για την ακεραία και σίγουρη μετάδοση των δεδομένων από το ένα άκρο στο άλλο. Το πλέον διαδεδομένο πρωτόκολλο αυτού του τύπου είναι το TCP (Transmission Control Protocol) που, σε στενή συνεργασία με το IP (Internet Protocol), αποτελεί τον κορμό του Internet. Το πέμπτο επίπεδο στην ιεραρχία (Application Layer, στην κορυφή της στοιβας) είναι άλλο ένα επίπεδο-κλειδί για τη λειτουργία ενός firewall. Το χρησιμοποιούν οι πόσες φύσας δικτυακές εφαρμογές, προκειμένου να επικοινωνούν (δικτυακά) μεταξύ τους και να παρέχουν τις υπηρεσίες τους σε προγράμματα-πελάτες.

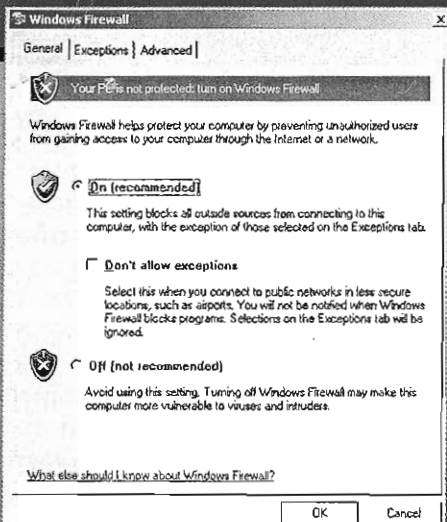
■ Το Α αλλά όχι και το Ω

Η παρουσία ενός firewall, σε οποιαδήποτε μορφή, αποτελεί επιτακτική ανάγκη για τους χρήστες που ενδιαφέρονται έστω και στο ελάχιστο για την ασφάλεια των δεδομένων ή την ακεραιότητα λειτουργίας των υπολογιστών τους και δεν αφήνουν τα πράγματα στην τύχη. Πόσο μάλλον τώρα που, με τις συνδέσεις DSL να πληθαίνουν διαρκώς, τα μηχανήματα παραμένουν πολλαπλάσιο χρόνο συνδεδεμένα –και συνεπώς εκτεθειμένα– στο Internet. Όμως η άμυνα ενός υπολογιστή δεν σταματά σε ένα καθορισμένο firewall. Δυστυχώς, η φύση των κινδύνων που απειλούν τα δεδομένα και την ψυχική μας ηρεμία ποικίλλει. Το firewall μπορεί να φανεί αρκετό για να εμποδίσει μια πιθανή εισβολή στον υπολογιστή μας, δεν θα μας προστατέψει όμως από έναν ιό που... κληρονομήσαμε από ένα πρόγραμμα που κλεβόμαστε κατεβάσαμε, χωρίς να γνωρίζουμε τι έμελλε να πάθουμε. Η ύπαρξη ενός καλού αντι-ιικού, λοιπόν, είναι κάτι παραπάνω από επι-

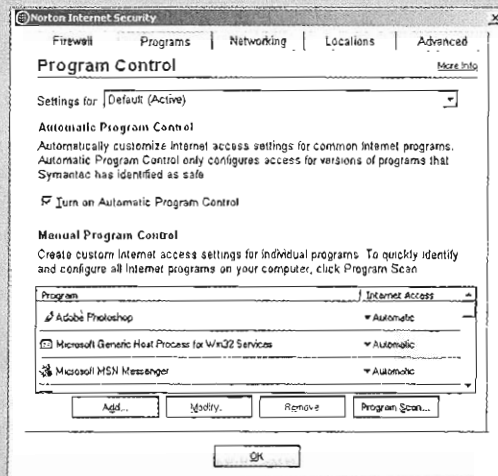
Ένα firewall που λειτουργεί σε αυτό το επίπεδο είναι σε θέση να αναλύει τα δεδομένα (payload) των πακέτων σε όσο το δυνατόν μεγαλύτερο βάθος.

«ΣΚΛΗΡΑ» FIREWALL. Ο λόγος γίνεται για τα λεγόμενα hardware firewall. Παρ' όλο που υπάρχουν και ως μεμονωμένες, εξειδικευμένες συσκευές, πλέον τα βρίσκουμε ενσωματωμένα και στο ADSL modem/router, που ήδη έχουν κατακλύσει την αγορά¹. Το γεγονός ότι με τη σύνδεση ADSL συνηθίζουμε και αφήνουμε τον υπολογιστή μας «εκτεθειμένο» στο Internet πολλαπλάσιο χρόνο σε σχέση με παλαιότερα κάνει επιτακτική την ανάγκη ύπαρξης ενός πρώτου αναχώματος προστασίας για τον υπολογιστή ή το τοπικό μας δίκτυο. Με βάση όσα αναφέραμε για τα επίπεδα του TCP/IP stack γίνεται φανερό ότι ένα hardware firewall θαμβάνει δράση στο τρίτο επίπεδο (Network Layer), φιλτράροντας τα πακέτα με κριτήρια όπως οι διευθύνσεις αποστολέα και παραλήπτη, οι θύρες, τα πρωτόκολλα μεταφοράς (π.χ., TCP, UDP, ICMP), καθώς και με συνδυασμούς αυτών. Ο συγκεκριμένος τρόπος ελέγχου είναι ο πλέον παραδοσιακός και ονομάζεται Packet Filtering. Πηγαίνοντας ένα βήμα παραπέρα, τα περισσότερα hardware firewall εφαρμόζουν την τεχνική SPI (Stateful Packet Inspection), η οποία προσδίδει στο firewall ένα βαθμό νοημοσύνης. Σύμφωνα με αυτή, το firewall είναι ικανό να αντιληφθεί πότε ένα τυχαίο πακέτο είναι μέρος μιας υπάρχουσας «συνομιλίας» μεταξύ δύο υπολογιστών. Έτσι, παραμένει «σφραγισμένο» σε οποιαδήποτε μορφή εισερχόμενη κίνηση που δεν ζητήθηκε από «μέσω», ενώ την ίδια στιγμή είναι «ανοιχτό» για την εξερχόμενη κυκλοφορία. Όταν ο υπολογιστής ζητήσει να δει, π.χ., μια σελίδα, ξεκινά μια συνομιλία με έναν απομακρυσμένο διακομιστή στέλνοντάς του την ανάλογη αίτηση. Το firewall, από την πλευρά του, επιτρέπει τη διακίνηση μόνο στα πακέτα που είναι μέρος αυτής –και μόνο αυτής– της συνομιλίας. Στο σημείο αυτό οφείλουμε να επισημάνουμε ότι

βεβλημένη. Και να ήταν μόνο αυτό! Στην παραβίαση του προσωπικού μας απορρήτου και στην επιβάρυνση της εύρυθμης λειτουργίας του συστήματος συμβάλλουν και τα λεγόμενα spy-ware. Πρόκειται για μικρά προγράμματα που συνήθως έρχονται μαζί με δοκιμαστικές ή δωρεάν εκδόσεις άλλων προγραμμάτων (τρανζακτό παράδειγμα αποτελεί η επίσημη έκδοση του Kazaa). Σκοπός τους είναι να καταγράφουν τις συνήθειές μας, όπως τις σελίδες που επισκεπτόμαστε, και στέλνουν κρυφά τις αναφορές τους σε τρίτους. Κατά πάσα πιθανότητα, ένα καθορυθμισμένο firewall θα αποτρέψει τη λειτουργία ενός spy-ware, ακόμα και αν αυτό χρησιμοποιεί κάποια άλλη «νομότυπη» εφαρμογή για να κάνει τη δουλειά του. Όμως γιατί να αφήνουμε τα spy-ware να δρουν ανεπόκητα στον υπολογιστή μας; Ένα καλό anti-spyware θα τα βρει και θα τα εξουδετερώσει. Περισσότερα για όλα αυτά θα δούμε στη συνέχεια του παρόντος αφιερώματος.



Το Windows XP προσφέρουν τη δική τους λύση personal firewall, η οποία μετά το Service Pack 2 εμφανίζεται αρκετά βελτιωμένη σε σχέση με την προγενέστερη έκδοση. Έχει όμως και ένα σημαντικό μειονέκτημα: Δεν πραγματοποιεί κανέναν απολύτως έλεγχο στην εξερχόμενη κίνηση (outbound traffic). Πιθανότατα πρόκειται για συνειδητή απόφαση της Microsoft, αφού, αν το firewall έλεγχε και την εξερχόμενη κίνηση, τότε ο χρήστης θα «ενοχλούνταν» διαρκώς από παράθυρα pop-up.



Όπως σε κάθε personal firewall, έτσι και στο Norton Personal Firewall μπορούμε να φτιάξουμε μια λίστα με τα προγράμματα που επιθυμούμε να έχουν επαφή με το Internet. Μπορούμε μάλιστα να διατηρούμε διαφορετικά προφίλ, με διαφορετικές λίστες προγραμμάτων και κανόνων, ανάλογα με το περιβάλλον στο οποίο βρισκόμαστε (π.χ., σπίτι, δουλειά).

ένο hardware firewall δεν μπορεί να κάνει κανέναν απολύτως έλεγχο στα δεδομένα αυτά καθαυτά (στο payload του πακέτου). Παρά το γεγονός αυτό, όμως, η ύπαρξή του είναι αναγκαία ως μια πρώτη γραμμή άμυνας, αφού –αν μη τι άλλο– μπορεί και κόβει «ύποπτα» πακέτα πριν καν αυτά φτάσουν στον υπολογιστή ή στους υπολογιστές πίσω από το firewall.

Η ΣΚΥΤΑΛΗ ΣΤΑ PERSONAL (SOFTWARE) FIREWALL. Ας υποθέσουμε ότι μια μέρα, χωρίς καλή καλή να το πάρουμε είδηση, κατεβάζουμε από το Internet (από εκείνους τους γνωστούς-άγνωστους δικτυακούς τόπους) ένα σχετικά επίφοβο πρόγραμμα, που τελικά αποδεικνύεται ένας δούρειος ίππος (trojan horse). Σκοπός αυτού του trojan μπορεί να είναι η συλλογή όποιου συνθηματικού βρίσκεται στο μηχανήμα από όπου τρέχει. Φυσικά, στην πρώτη ευκαιρία που θα βρει θα επικοινωνήσει με το απομακρυσμένο μηχανήμα κάποιου κακόβουλου –ή έστω υπέρ το δέον «περίεργου»– χρήστη, ώστε να του αποστείλει τα ευρήματά του (τους κωδικούς μας!). Τώρα ο δημιουργός του trojan έχει ήδη προβλέψει την παρουσία hardware firewall μπροστά από τα μηχανήματα των «θυμάτων», επομένως έχει φτιάξει το trojan ώστε να επικοινωνεί μέσω της θύρας 80: Αυτή τη θύρα τη χρησιμοποιούν όλα τα προγράμματα πλοήγησης, επομένως το firewall είναι λογικό να επιτρέπει την επικοινωνία μέσω αυτής. Καλή μοντέψατε, σε ένα τέτοιο –διόλου απίθανο– σενάριο, οι πολύτιμοι κωδικοί μας έχουν πέσει σε ξένα χέρια!

Κάπου εδώ αναλαμβάνει ρόλο στενότερου «μαρκαρίσματος» το personal ή software firewall. Δρώντας στο Application Layer του TCP/IP stack, ένα τέτοιο firewall είναι σε θέση να περνά από το μικροσκόπιο όλα τα δεδομένα που διακινούνται από και προς το μηχανήμα που προστατεύει. Μάλιστα οι τεχνικές φιλτραρίσματος που εφαρμόζουν τα firewall της κατηγορίας χαρακτηρίζονται από την πολυπλοκότητα αλλά και από τη μεγάλη αποτελεσματικότητά τους. Πολλά personal firewall, για παράδειγμα, παρέχουν τη δυνατότητα κατάρτισης μιας λίστας με αφαιρεσιμικά που δεν πρέπει σε καμία απολύτως περίπτωση να βγαίνουν από τον υπολογιστή μας. Αυτή η λίστα ενδέχεται να περιλαμβάνει κωδικούς, αριθμούς πιστωτικών καρτών και άλλα αυστηρώς προσωπικά δεδομένα. Σε περίπτωση, λοιπόν, που κάποιο κακόβουλο πρόγραμμα, όπως το trojan του παραδείγματος, προσπαθήσει να στείλει προς τα «έξω» κάποια από αυτές τις πληροφορίες, το personal firewall αφυπνίζεται και εμποδίζει την αποστο-

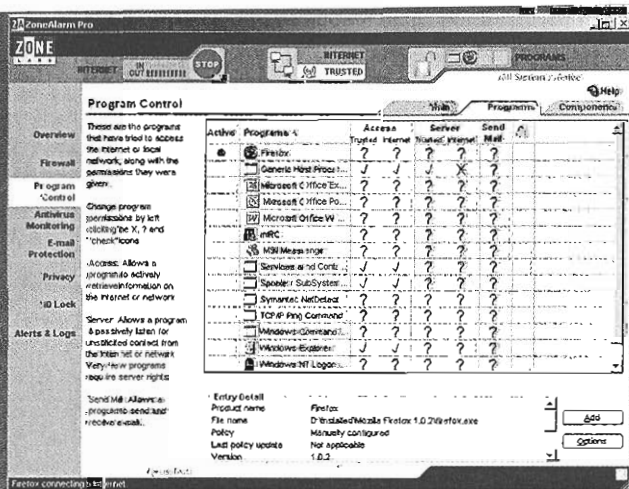
λή τους. Ωστόσο, η πλέον αξιοσημείωτη δυνατότητα των personal firewall αφορά στον έλεγχο ξεχωριστών εφαρμογών. Τα firewall της κατηγορίας είναι γραμμένα για συγκεκριμένα λειτουργικά συστήματα. Το γεγονός αυτό επιτρέπει τη δημιουργία λιστών με τα δικαιώματα πρόσβασης στο Internet καθεμιάς εκ των εφαρμογών που δουλεύει ο χρήστης. Σε μια τέτοια λίστα, για παράδειγμα, το Mozilla Firewall και ο Internet Explorer θα έχουν πλήρη πρόσβαση στο Internet. Εάν ένα πρόγραμμα βρίσκεται ήδη στη λίστα και του έχει απαγορευτεί η αποστολή πακέτων στο Internet (εξερχόμενη κυκλοφορία, outbound traffic), δεν θα μπορέσει να στείλει τίποτε έξω, ακόμη και αν χρησιμοποιεί τη θύρα 80 (που χρησιμοποιούν τα Firefox και Explorer). Αν πάλη ένα πρόγραμμα περιλαμβάνεται στη λίστα και του έχει απαγορευτεί η λήψη πακέτων (εισερχόμενη κυκλοφορία, inbound traffic), κανένα πρόγραμμα από «έξω» δεν θα μπορέσει να επικοινωνήσει μαζί του, ακόμη και αν το επιχειρήσει από μία καθ' όλα νομότυπη και ανοιχτή θύρα. Ας υποθέσουμε, τέλος, ότι κάποιο πρόγραμμα δεν βρίσκεται στη λίστα δικαιωμάτων του software firewall. Την πρώτη φορά που θα επιχειρήσει να στείλει ή να δεχτεί κάποιο πακέτο προς ή από το Internet, το software firewall θα διακόψει αμέσως την επικοινωνία και θα ενημερώσει σχετικά το χρήστη (αρκεί, βέβαια, να είναι ενεργοποιημένο). Εκείνος, τότε, θα αποφασίσει εάν θα επιτρέψει ή όχι την επικοινωνία, για αυτή μόνο τη φορά ή για το μέλλον. Έτσι, την πρώτη φορά που το trojan του παραδείγματος μας επιχειρήσει να επικοινωνήσει με τον κακόβουλο χρήστη, ασχέτως αν χρησιμοποιήσει το port 80 ή οποιοδήποτε άλλο, ο ιδιοκτήτης του «προσβεβλημένου» υπολογιστή θα ενημερωθεί για την απόπειρα και θα κληθεί να επιτρέψει/απαγορεύσει στο πρόγραμμα την επικοινωνία, για αυτή μόνο τη φορά ή και για κάθε άλλη. Στην προσπάθειά του να βοηθήσει το χρήστη να λάβει τη σωστή απόφαση, το personal firewall θα του παρουσιάσει πλήθος βοηθητικών στοιχείων, όπως όνομα εφαρμογής, μέγεθος, θέση στο δίσκο, όνομα κατασκευαστή κ.ά.

Άλλο ένα χαρακτηριστικό που απαντάται σε αρκετά personal firewall είναι το λεγόμενο IDS (Intrusion Detection System, σύστημα εντοπισμού εισβολών – συναντάται και στα hardware

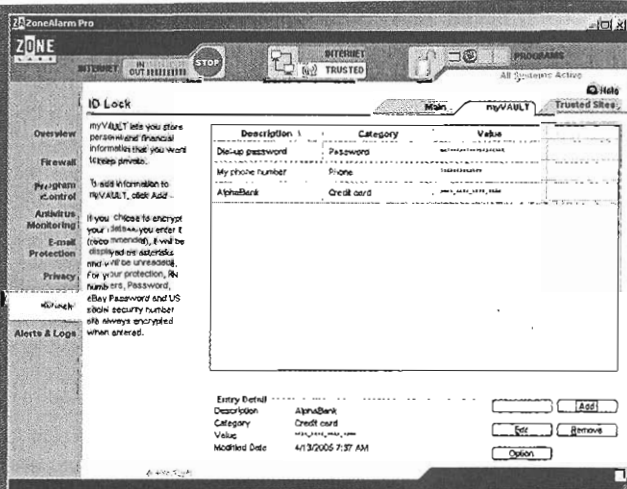
firewall]). Όποτε υπάρχει και είναι ενεργοποιημένο το IDS, το firewall διατηρεί μια βάση με συχνά χρησιμοποιούμενες τεχνικές διείσδυσης και υποκλοπής. Όταν «αντιληφθεί» ότι κάτι τέτοιο λαμβάνει χώρα, αντιδρά ανάλογα. Μάλιστα, καθώς νέες τεχνικές αναπτύσσονται από τους «αγήσικους» χρήστες του Διαδικτύου, οι βάσεις αυτές ερμηλοποιούνται και το personal firewall τις λαμβάνει από την κατασκευάστρια εταιρεία.

Κατά πώς φαίνεται, τα personal firewall δείχνουν να προσφέρουν την καλύτερη μορφή ελέγχου και προστασίας, όμως δεν παύουν να έχουν και αυτά τα μειονεκτήματά τους. Το κυριότερο είναι το γεγονός ότι συχνά γίνονται στόχος των cracker που προσπαθούν είτε να τα ξεγελάσουν είτε να τερματίσουν βίαια τη λειτουργία τους και να δράσουν έτσι ανενόχλητοι. Επίσης, ένα τυπικό personal firewall για Windows προστατεύει μόνο τον υπολογιστή στον οποίο βρίσκεται εγκατεστημένο και όχι όλη τη μηχανήματα του τοπικού δικτύου. Ακόμη και αν είναι εγκατεστημένο στον υπολογιστή-πύλη προς το Διαδίκτυο (Internet Gateway), δεν θα είναι σε θέση να ελέγχει τις εφαρμογές που τρέχουν στα υπολοίπα μηχανήματα του δικτύου.

Στο σημείο αυτό θα μπορούσε να σκεφτεί κανείς ότι η ύπαρξη περισσότερων από ένα personal firewall στον ίδιο υπολογιστή ενισχύει σημαντικά την προστασία του μηχανήματος. Και όμως, η ύπαρξη περισσότερων του ενός personal firewall στον ίδιο υπολογιστή είναι σχεδόν βέβαιο ότι θα προκαλέσει σοβαρές περιπλοκές και δυσλειτουργίες σε ολόκληρο το λειτουργικό σύστημα. Μόνο ένα personal firewall μπορεί –και πρέπει– να επεξεργάζεται τα διακινούμενα δικτυακά πακέτα. Τα παραπάνω ισχύουν και για το firewall που έρχεται με το SP2 των Windows XP: Δεν πρέπει να είναι ενεργοποιημένο, όταν ταυτόχρονα λειτουργεί και κάποιο τρίτο firewall.



Το ZoneAlarm είναι ιδανικό τόσο για τον απλίο όσο και για τον πιο προχωρημένο χρήστη. Ενώ ο πρώτος –στην αρχή και όποτε χρειάζεται κάποιο όγμα ασφαλείας– θα προχωρήσει στη ρύθμιση του firewall μέσα από μια σειρά ερωτηματολογίων, ο δεύτερος θα έχει και τη δυνατότητα χειροκίνητων ρυθμίσεων.



Ένα από τα σημαντικά χαρακτηριστικά του ZoneAlarm είναι η λειτουργία ID Lock. Με αυτή μπορούμε να φτιάξουμε μια λίστα με τα ευαίσθητα δεδομένα που μας αφορούν, όπως κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών και διευθύνσεις e-mail, ώστε κάθε φορά που ένα από αυτά τα στοιχεία πάσκει να «βγει» στο Internet, να ερωτώμαστε και να επιτρέπουμε ή να αποτρέπουμε την αποστολή του.

ΒΙΟΤΟΠΟΣ ΤΟ PC

Τα παιχνίδια με τον κώδικα μικρών και μεγάλων αλλά πάντα «ανώριμων» παιδιών φέρνουν σε εξαιρετικά δύσκολη θέση τόσο τον υπολογιστή και τα δεδομένα μας όσο και το Internet και τις υπηρεσίες του. Αλλά εμείς δεν πρόκειται να μείνουμε με σταυρωμένα τα χέρια.

ΕΝΑ «ΚΟΜΠΙΟΥΤΕΡΙΣΤΙΚΟ» ΡΗΤΟ επισημαίνει ότι εφόσον σε κάποιο μηχάνημα υπάρχει λειτουργικό σύστημα που επιτρέπει την εκτέλεση εφαρμογών, τότε το σύστημα αυτό είναι εξ ορισμού ευάλωτο σε ιούς. Εάν σε αυτό προσθέσουμε τη μεγάλη εξάπλωση του περί ου λόγος λειτουργικού συστήματος (ένα τυχαίο παράδειγμα αποτελούν τα Windows :) καθώς και τις πολλές και διάφορες προγραμματιστικές αδυναμίες που ενδέχεται να έχει, είναι προφανές ότι αμέσως αμέσως δημιουργείται ένα εξαιρετικά ελκυστικό περιβάλλον για ορισμένες ομάδες ανθρώπων, νεαρής συνήθως ηλικίας, οι οποίοι δεν έχουν κάτι καλύτερο να κάνουν στη ζωή τους από το να δυσκολεύουν τη δική μας. Οι ιοί, οι δούρειοι ίπποι και τα σκουλήκια είναι τα δημιουργήματα αυτών των ανθρώπων και αποτελούν προεξέχοντα μέλη της μεγάλης οικογένειας των κακόβουλων εφαρμογών (malware).

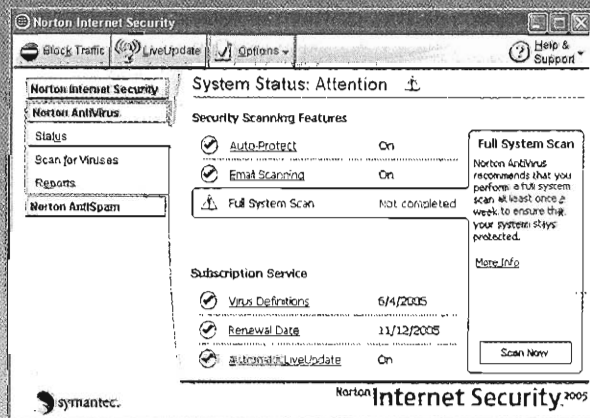
ΜΙΚΡΑ ΚΑΙ ΜΕΓΑΛΑ ΚΡΥΟΛΟΓΗΜΑΤΑ. Οι ιοί είναι μικρά προγράμματα τα οποία συνήθως χρησιμοποιούν συγκεκριμένες δυνατότητες που ενσωματώνει το εκάστοτε λειτουργικό σύστημα, με

σκοπό την αναπαραγωγή και την εξάπλωσή τους από υπολογιστή σε υπολογιστή. Σε κάθε μηχάνημα που θα «θρονοιστούν» θα φροντίσουν να κάνουν μία, δύο ή πολύ περισσότερες ζημιές. Συνήθως οι ιοί έρχονται προσκολλημένοι σε κάποια «νομιμοφανή» εφαρμογή, ούτως ώστε να ρίξουν στάχτη στα μάτια του χρήστη. Φυσικά, με το που εκτελείται η εφαρμογή-ξενιστής, ο ιός σπεύδει να μολύνει το σύστημα. Ο εκτελέσιμος κώδικας των ιών συνήθως έχει τη μορφή κάποιου αρχείου με κατάληξη .exe, αλλά μπορεί να καλυφθεί κάτω από το «μανδύα» μιας εικόνας .jpg ή ενός .mp3, για παράδειγμα. Άλλοτε ένας ιός θα επιχειρήσει να εισχωρήσει στο μηχάνημά μας ως συνημμένο αρχείο σε κάποιο e-mail. Ακόμη και μια απλή περιήγηση σε «παράξενους» δικτυακούς τόπους όμως είναι πολύ πιθανό να γίνει αιτία μόλυνσης από ιό ή από άλλο κακόβουλο πρόγραμμα (περισσότερα γι' αυτά σε λίγο).

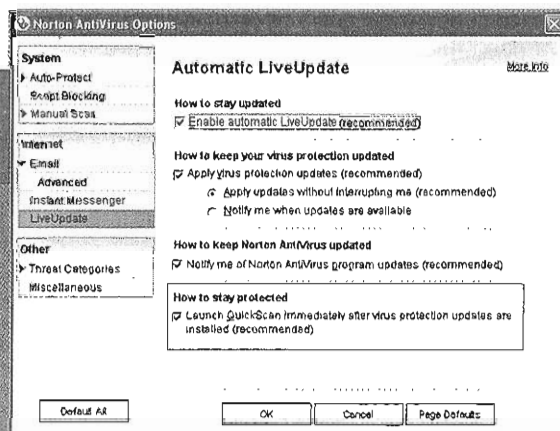
Οι επιπτώσεις στο σύστημα που μολύνεται μπορεί να είναι από αμελητέες έως καταστροφικές. Για παράδειγμα, ο δημιουργός του ιού πιθανόν να θέλει το δημιούργημά του απλώς να πωληθεί, πηλασιάζεται και να εξαπλώνεται ή, στη χειρότερη περίπτωση,

Norton AntiVirus

Το Norton AntiVirus της Symantec είναι μια εμπορική εφαρμογή που πωλείται είτε αυτόνομα είτε μαζί με σουίτες εφαρμογών, όπως, για παράδειγμα, το Norton Internet Security και Norton Systemworks.



Το κεντρικό παράθυρο ελέγχου της εφαρμογής. Το σύστημα ενημέρωσης του χρήστη είναι πολύ καλό, καθώς ο χρωματισμός απεικονίζει ανάλογα με την κατάσταση. Για παράδειγμα, κινδυνεύει εφόσον δεν έχει ολοκληρωθεί μια ενέργεια ή κοκκινίζει όταν λήξει η περίοδος λήψης ενημερώσεων για τον εντοπισμό ιών.



Η καθημερινή ενημέρωση των βάσεων αναγνώρισης κακόβουλων εφαρμογών, μέσω Internet, είναι κάτι παραπάνω από αναγκαίο για να έχουμε πάντα την καλύτερη δυνατή προστασία για κάθε απειλή. Στο κάτω μέρος διακρίνεται η επιλογή για γρήγορο έλεγχο του υπολογιστή έπειτα από κάθε ενημέρωση. Σε τακτά χρονικά διαστήματα θα πρέπει να διενεργείται και πλήρης έλεγχος παρά το σχετικά μεγάλο χρόνο που απαιτεί.

να καταστρέφει αρχεία και δεδομένα στο σκληρό δίσκο του θύματος, με τυχαία κριτήρια ή όχι. Παρεμπιπτόντως, η τακτική λήψη αντιγράφων ασφαλείας κρίσιμων αρχείων και πληροφοριών ενδέχεται να μας γλιτώσει από μελλοντικούς μελάνδες και δυσάρεστες περιπτώσεις.

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες, γενικές κατηγορίες.

- **Ιοί αρχείων και εκκίνησης συστήματος.** Οι πιο διαδεδομένοι ιοί είναι αυτοί που χρησιμοποιούν το σύστημα αρχείων των Windows για να εξαπλωθούν και είτε εγκαθίστανται σε κάποιο μέρος του σκληρού δίσκου είτε μολύνουν κάποιο υπάρχον αρχείο, με τον παράτυπο κώδικά τους. Οι ιοί εκκίνησης συστήματος μολύνουν το master boot record του σκληρού δίσκου, με συνέπεια να εκτελούνται κάθε φορά που γίνεται εκκίνηση του συστήματος. Οι ιοί εκκίνησης συστήματος είναι σχετικά σπάνιοι σήμερα. Αντίθετα, οι δημιουργοί ιών τούς φτιάχνουν με τέτοιον τρόπο, ώστε συνήθως να διαδίδονται ως συνημμένα ηλεκτρονικής αλληλογραφίας.

- **Ιοί macro/script.** Οι γλώσσες macro χρησιμοποιούνται σε εφαρμογές όπως το Word ή το Excel, για την αυτοματοποιημένη εκτέλεση πλήθους ενεργειών, π.χ., με το άνοιγμα ενός αρχείου. Με κατάλληλη «χειραγώγηση» των γλωσσών macro είναι δυνατή η δημιουργία των λεγόμενων «μακροϊών», οι οποίοι συχνά επιφέρουν δυσάρεστες και μη αντιστρεπτές τροποποιήσεις στα έγγραφα μας. Ένας αρκετά γνωστός ιός macro ήταν ο Melissa, ο οποίος μόλυνε το αρχείο Normal.dot του Word και εξαπλωνόταν μέσω e-mail. Οι δέσμες ενεργειών (script) της Visual Basic ή της Java (Javascript) μπορούν επίσης να χρησιμοποιηθούν κακόβουλα, προκειμένου να εκτελεστεί επικίνδυνος κώδι-

Τον τελευταίο καιρό μεγάλη άνθηση γνωρίζουν και οι ιοί για Smartphones, με λειτουργικό σύστημα Symbian OS ή Windows Mobile. Τα Smartphone επιτρέπουν την εγκατάσταση και την εκτέλεση εφαρμογών, με συνέπεια να αποτελούν πρόσφορο έδαφος για ιούς. Παράλληλη άνθηση παρουσιάζουν και τα αντιβιοτικά για Smartphone. Σε γενικές γραμμές, μεγάλη προσοχή θα πρέπει να δείχνετε σε άγνωστα αρχεία που λαμβάνετε μέσω Bluetooth ή MMS.

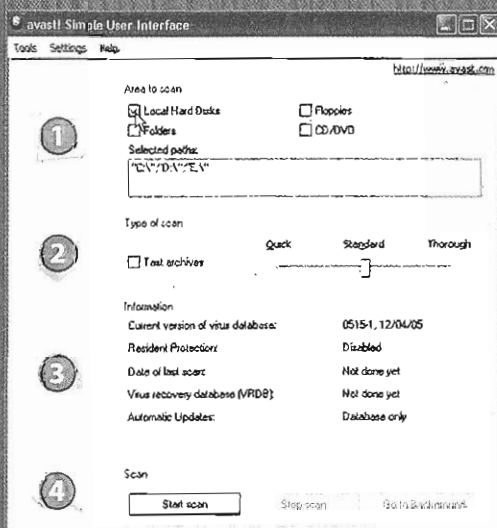
κας στον υπολογιστή, φυσικά χωρίς την έγκρισή μας.

Δύο είναι τα βασικά αντίμετρα κατά των ιών: Η ύπαρξη ενός αντι-ιικού προγράμματος στον υπολογιστή μας, το οποίο θα πρέπει να ενημερώνεται τακτικά από το Internet με τις υπογραφές αναγνώρισης ιών, καθώς και η λήψη/εγκατάσταση των κρίσιμων ενημερώσεων του λειτουργικού, μέσω του Windows Update. Τα δε αντι-ιικά προσφέρουν προστασία σε πραγματικό χρόνο, έτσι ώστε να μειώνεται η πιθανότητα μόλυνσης από ιό που βρίσκεται σε κάποιο αρχείο που κατεβάζουμε ή προσπαθεί να παρεισφρήσει στο μηχανήμα από ένα πρόγραμμα instant messaging. Ο εβδομαδιαίος (τουλάχιστον) πλήρης έλεγχος όλων των δίσκων του μηχανήματος αποτελεί άλλο ένα αναγκαίο μέτρο.

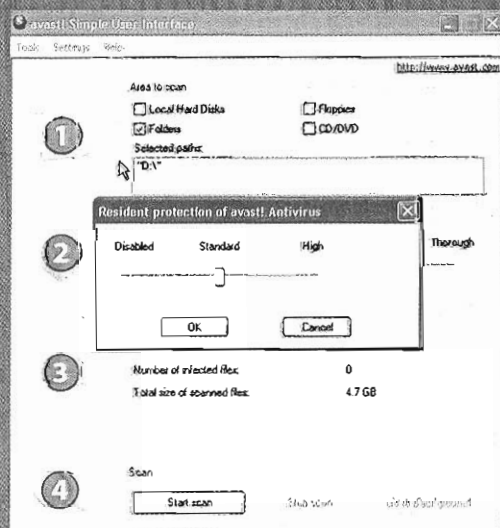
ΑΠΟ ΤΗΝ ΤΡΟΙΑ ΜΕ ΑΓΑΠΗ. Οι δούρειοι ιπποί (trojan horses) είναι εξαιρετικά επικίνδυνες εφαρμογές οι οποίες κάνουν ό,τι μπορούν για να εξαπατήσουν το χρήστη, έτσι ώστε να τις εκτελέσει και να υποβαθμίσουν την ασφάλεια του PC. Συνήθως κρύβονται πίσω από κάποια φαινομενικά αθώα εφαρμογή και είναι ικανοί, μεταξύ άλλων, να μολύνουν το σύστημα με κάποιο ιό, να συλλέξουν προσωπικά στοιχεία, να χρησιμοποιήσουν τον υπολογιστή μας για απομακρυσμένες επιθέ-

■ avast! Antivirus

Η Alwil Software έχει μια ενδιαφέρουσα στρατηγική για το avast! Antivirus. Το προσφέρει σε δύο εκδόσεις. Η Home προσφέρεται δωρεάν, με την εταιρεία να ζητά μια εγγραφή στο δικτυακό τόπο www.avast.com. Η έκδοση Pro προσφέρει περισσότερες δυνατότητες για πιο έμπειρους χρήστες, όπως, για παράδειγμα, η επιτήρηση του Office, εφαρμογών Peer to Peer, και διαφορετικό περιβάλλον εργασίας.



Το περιβάλλον εργασίας του avast! Home είναι εξαιρετικά απλό και καθοδηγεί το χρήστη, με τέσσερα ξεκάθαρα βήματα, για την πραγματοποίηση ελέγχου και το ξεκαθάρισμα των ιών.



Ο έλεγχος του συστήματος σε πραγματικό χρόνο για ιούς δεν είναι ενεργοποιημένος εξ αρχής. Θα πρέπει να τον ενεργοποιήσετε από το μενού των ρυθμίσεων, καθώς πρόκειται για βασικό μέτρο προφύλαξης.

σεις, ακόμη και να επιτρέψουν σε τρίτους να έχουν πλήρη πρόσβαση στον υπολογιστή μας. Υπάρχουν αρκετά είδη δούρειων ίππων, με πιο επικίνδυνους τους παρακάτω:

- **Κερκόπορτες (Backdoors).** Ο υπολογιστής που έχει μολυνθεί με ένα τέτοιο trojan είναι ανοιχτός για πλήρη έλεγχο από τον επιτιθέμενο (διαγραφή αρχείων, απομακρυσμένη εκτέλεση εφαρμογών, απομακρυσμένος τερματισμός κ.ά.), μερικές φορές μάλιστα χωρίς το «θύμα» να είναι σε θέση να καταλάβει τι ακριβώς συμβαίνει.

- **Υποκλινοί δεδομένων.** Πραγματοποιούν αναλυτικούς ελέγχους του προσβεβλημένου συστήματος έτσι ώστε να βρουν, π.χ., αριθμούς πιστωτικών καρτών και άλλα ευαίσθητα προσωπικά δεδομένα. Μόλις εντοπίσουν κάτι, στέλνουν τα ευρήματά τους στον επιτιθέμενο, π.χ., μέσω e-mail, ήσυχια και αθόρυβα.

- **Προπομποί ιών (Downloaders-Droppers).** Όταν ένα trojan της κατηγορίας μολύνει έναν υπολογιστή, ειδοποιεί τον επιτιθέμενο ότι έχει ανοίξει το δρόμο για εγκατάσταση άλλων κακόβουλων εφαρμογών, όπως, για παράδειγμα, ιών.

- **Μεσάζοντες επιθέσεων (Zombie-Proxy).** Σε αυτή την περίπτωση ο δούρειος ίππος μετατρέπει τον υπολογιστή μας σε διακομιστή μεσοδόθησης (proxy), εν αγνοία μας φυσικά, με συνέπεια τη χρήση του για συγκεκαλυμμένες επιθέσεις σε τρίτους υπολογιστές ή δίκτυα.

Για την αντιμετώπιση των δούρειων ίππων χρειάζεται η παρουσία ενός συνόλου εφαρμογών προστασίας/καταστολής. Ενημερωμένα αντι-ιικά και anti-spyware θεωρούνται απαραίτητα, αφού με τον τρόπο αυτό αναπτύσσουμε την άμυνά μας για όσο το δυνατόν περισσότερα είδη δούρειων ίππων. Φυσικά, σε τακτά χρονικά διαστήματα θα πρέπει να πραγματοποιούνται πλήρεις, εξονυχιστικοί έλεγχοι του υπολογιστή. Η ύπαρξη software firewall είναι επίσης εξαιρετικά χρήσιμη,

■ Αντιβιοτικά για όλους

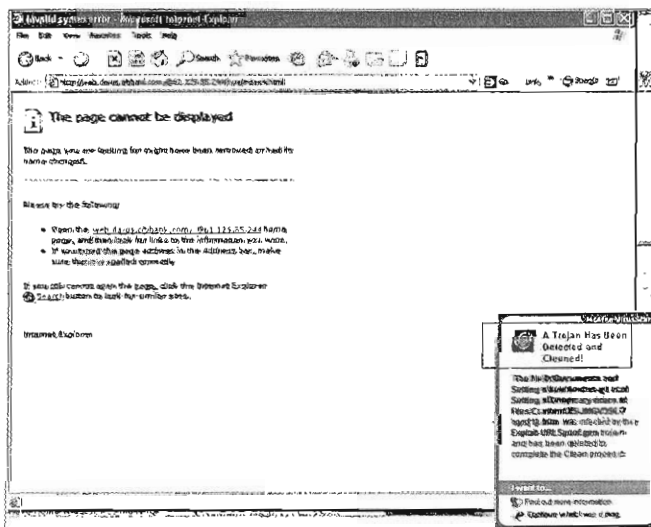
AntiVirusKit 2005 Professional	www.antispyware.com	35,95€
Avast! 4 Professional	www.avast.com	35,95€
AVG Professional	www.grisoft.com	33,30€
BitDefender 8 Standard	www.bitdefender.com	23€
ClamWin Antivirus 0.83	www.clamwin.com	δωρεάν
Dr.Web Antivirus 4.32b	www.drweb.com	24,90€
eTrust EZ Antivirus 2005	www.ca.com	23€
F-Prot Antivirus	www.f-prot.com	22€
F-Secure Antivirus 2005	www.f-secure.com	63€
Kaspersky Anti-virus Personal 5.0	www.kaspersky.com	32€
McAfee Viruscan 2005	www.mcafee.com	49,98€
Nod32 2.12	www.nod32.com	37,38€
Norton Antivirus 2005	www.symantec.com	38,4€
Panda Titanium Antivirus 2005	www.pandasoftware.com	49,95€
TrendMicro PC-cillin 12	gr.trendmicro-europe.com	59€
ZoneAlarm Antivirus	www.zonelabs.com	30€

Στην αγορά κυκλοφορούν δεκάδες προϊόντα κατά ιών, σκουληκιών και δούρειων ίππων, τα οποία είτε προσφέρονται αυτόνομα είτε είναι μέρος κάποιας σουίτας που περιλαμβάνει, π.χ., και firewall. Τις εφαρμογές μπορείτε να τις αγοράσετε και να τις κατεβάσετε από τους δικτυακούς τόπους των κατασκευαστών, ενώ μερικές από αυτές φυσικά προσφέρονται σε «κανονική» συσκευασία στα καταστήματα. Τα βασικά σημεία επιλογής αντι-ιικών είναι η δυνατότητα ελέγχου σε πραγματικό χρόνο, οι συχνές ενημερώσεις, ο έλεγχος εισερχόμενων/εξερχόμενων e-mail, αρχείων που κατεβαίνουν από προγράμματα messenger και P2P, καθώς και η παροχή ενημερώσεων ασφάλειας από την κατασκευαστική εταιρεία. Οι παραπάνω τιμές αφορούν στις εκδόσεις τις οποίες μπορείτε να αγοράσετε ή να κατεβάσετε από το Internet και συνήθως περιλαμβάνουν μια άδεια χρήσης και 12 μήνες υποστήριξη. Στην περίπτωση του AVG Antivirus προσφέρεται 24μην υποστήριξη/ανανέωση της βάσης αναγνώρισης ιών. Το ZoneAlarm Antivirus περιλαμβάνει και firewall. Το ClamWin Antivirus αποτελεί ανοικτό λογισμικό.

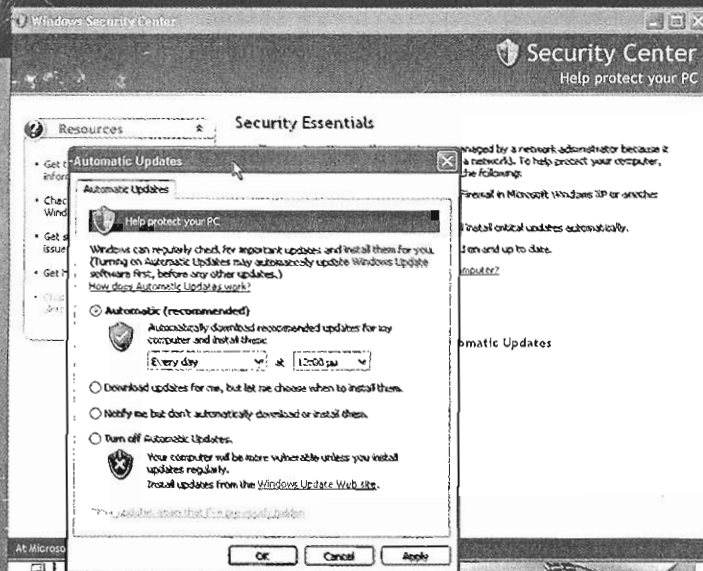
για δύο λόγους. Κατ' αρχάς, το πρόγραμμα ειδοποιεί το χρήστη κάθε φορά που μια αναξιόπιστη εφαρμογή επιχειρεί να βγει στο Internet, εμποδίζοντας την επικοινωνία της έως ότου ο χρήστης το επικρίψει ή το απαγορεύσει. Περισσότερο να πούμε ότι ο τελευταίος πρέπει να γνωρίζει τι κάνει. Δεύτερον, εάν το firewall είναι κατάλληλα ρυθμισμένο, θα ειδοποιήσει το χρήστη ακόμη και όταν το trojan χρησιμοποιήσει κάποια άλλη, έμπιστη εφαρμογή για να επικοινωνήσει με τον έξω κόσμο.

ΛΑΘΡΑΙΟΙ ΤΑΞΙΔΙΩΤΕΣ. Τα λεγόμενα δικτυακά σκουλήκια (worms) έχουν μοναδικό σκοπό τη μετάδοση-εξόπλησή τους σε πάσης φύσεως δικτυακούς κόμβους (κάθε υπολογιστής που συνδέεται στο Internet αποτελεί ενεργό κόμβο του, ανεξάρτητα από το εάν είναι διακομιστής ή όχι). Σε κάθε μηχανήμα που καταφτάνουν, πριν επιχειρήσουν να μεταφερθούν σε κάποιο άλλο, πιθανότατα θα προκαλέσουν ζημιά ή θα δημιουργήσουν προβλήματα στην ομαλή λειτουργία του. Επίσης, ένα worm ενδέχεται να είναι προγραμματισμένο ώστε σε συγκεκριμένη ημερομηνία και ώρα να εξαπολύσει —εκείνο και κάθε αντίγραφο του— μια επίθεση DDOS (Distributed Denial of Service) σε συγκεκριμένο διακομιστή.

Για τη διακίνησή τους τα σκουλήκια εκμεταλλεύονται μία ή περισσότερες δικτυακές υπηρεσίες, όπως το file sharing των Windows ή/και το e-mail. Ένας άλλος τρόπος εξόπλησης



Δούρειος ίππος υψηλού κινδύνου ο οποίος αναχαιτίστηκε εγκαίρως. Έχει στόχο να παραπλανήσει τον χρήστη αφού εμφανίζεται να προέρχεται από μια γνωστή τράπεζα και ζητά από το χρήστη να επισκεφθεί μια συγκεκριμένη σελίδα και να εισαγάγει τα στοιχεία εισόδου στο Web Banking που τυχόν είναι συνδρομητής. Για κανένα λόγο δεν θα πρέπει να αποκαλύπτετε ευαίσθητα προσωπικά στοιχεία ύστερα από αιτήσεις μέσω e-mail ή τηλεφωνικά.



Note: You must be logged on to your computer with an account that is part of the Administrators group to run this tool.

Scan and Clean Your PC

1. Verify Your Windows Version

This tool works only on Microsoft Windows XP, Windows 2003, and Windows Server 2003. If you are not sure which version of Windows you are running, review instructions for how to check.

2. Run the Removal Tool

This tool scans your hard disk for viruses and tries to remove them. To proceed, click Check My PC for Infection.

Check My PC for Infection

Note: To use this tool, you must agree to the terms of the end user license agreement. Your computer may also display a warning that the tool is attempting to run; click Yes to proceed.

Note: If you have difficulty running the tool from this page, it may be due to your browser's security settings. If you have any problems, try downloading the tool directly from the Microsoft.com Download Center and then running it manually.

Απαιτείται: Μετά την προσθήκη του Service Pack 2 στα Windows XP, το κέντρο ασφαλείας αναλαμβάνει να ενημερώνει το χρήστη για διάφορα θέματα προστασίας από κακόβουλες εφαρμογές. Δεξιά: Η Microsoft, αναγνωρίζοντας το πρόβλημα με τους ιούς που μας περιτριγυρίζουν, διαθέτει μέσω του Windows Update ένα καθαριστικό εργαλείο για αρκετές κακόβουλες εφαρμογές.

είναι μέσω ActiveX και JavaScript, όπου ο χρήστης μοιράζεται αφού επισκεφθεί κάποιο –συνήθως περίεργο ή/και περιφερειακό– δικτυακό τόπο και δεχτεί το κατέβασμα λογισμικού, το οποίο υποτίθεται ότι επανυξάνει τις δυνατότητες του προγράμματος πληροφόρησης κ.λπ. Υπάρχουν ακόμη σκουλήκια που για την εξάπλωσή τους εκμεταλλεύονται το προγράμμα-τα άμεσας επικοινωνίας (instant messaging, MSN, ICQ κ.ά.).

Όπως προαναφέραμε, για την εξάπλωσή τους τα σκουλήκια εκμεταλλεύονται διάφορες αδυναμίες των Windows, καθώς και άλλες δικτυακές υπηρεσίες. Ως εκ τούτου, η τακτική εγκατάσταση των κρίσιμων ενημερώσεων των Windows είναι ένα βασικό μέτρο προφύλαξης. Σε δεύτερο επίπεδο, ένα αντι-ιικό θα πρέπει να είναι παρόν στον υπολογιστή, πάντα με ενημερωμένες τις υπογραφές ανίχνευσης κακόβουλων προγραμμάτων. Επίσης, το firewall είναι δυνατόν να αποτρέψει την περαιτέρω εξάπλωση ενός worm.

MICROSOFT MALICIOUS SOFTWARE REMOVAL. Οι δημιουργοί αντι-ιικών παρουσιάζουν συνεχώς εργαλεία καθαρισμού για συγκεκριμένους ιούς και σκουλήκια. Για παράδειγμα, στη διεύθυνση securityresponse.symantec.com/avcenter/tools.list.html θα βρείτε μια μεγάλη λίστα από καθαριστικά συγκεκριμένων ιών και σκουληκιών, ελεύθερα για να τα κατεβάσετε και να τα χρησιμοποιήσετε. Οι περισσότεροι από εσάς θα έχετε ήδη παρατηρήσει ότι οι πρόσφατες ενημερώσεις του Windows Update περιλαμβάνουν την εφαρμογή Malicious Software Removal. Πρόκειται για ένα «ομαδικό καθαριστικό» της Microsoft, για αρκετούς γνωστούς ιούς και σκουλήκια. Για να το χρησιμοποιήσετε θα πρέπει, με τον Internet Explorer, να επισκεφθείτε τη διεύθυνση www.microsoft.com/security/malwareremove/default.msp. Ανά τακτά χρονικά διαστήματα η εφαρμογή ενημερώνεται, έτσι ώστε να καθαρίζει ακόμη περισσότερα και νέα κακόβουλα προγράμματα. Να διευκρινίσουμε ότι οι εφαρμογές αυτές είναι εξαιρετικά χρήσιμες εφόσον έχετε κολλήσει συγκεκριμένους ιούς και φυσικά τους έχετε εντοπίσει με κάποιο τρόπο. Είναι πιθανόν, π.χ., το αντι-ιικό σας να έχει εντοπίσει τον ιό, αλλά να μην ήταν σε θέση να τον καθαρίσει. Εντοπισμός μπορεί να γίνει και ύστερα από έναν έλεγχο on-line.

SECURITY CENTER ΤΩΝ WINDOWS XP SP2. Με την έλευση του Service Pack 2 των Windows XP αλλά και με την εφαρμογή Anti-Spyware (την οποία απέκτησε η Microsoft μετά την εξαγορά της Giant, www.giantcompany.com), έστω και καθυστερημένα η Microsoft δείχνει την «ευαισθησία» της στη στρατιά των κακόβουλων εφαρμογών που μας απειλούν. Το Service Pack 2 κλείνει πολλή κενά ασφαλείας των Windows, με το Security Center να ελέγχει εάν υπάρχουν εγκατεστημένα αντι-ιικά και firewall στον υπολογιστή, καθώς και αν το πρώτο είναι ενημερωμένο. Επίσης οναλαμβάνει την εύκολη διαχείριση των αυτόματων ενημερώσεων, από το Windows Update.

Άλλη μια φορά θα πρέπει να σταθούμε στο Windows Update και στη μεγάλη σημασία των ενημερώσεων ασφαλείας των Windows, για την ασφαλεία του συστήματός μας. Ο σχετικός μεγάλος χρόνος που μερικές φορές απαιτείται για το κατέβασμα των ενημερώσεων, σε συνδέσεις dial-up 56K, αξίζει τον κόπο και με το παραπάνω θα λέγαμε. Στη διεύθυνση www.microsoft.com/hellas/athome/security θα βρείτε αρκετές πληροφορίες και παραπομπές για μια μεγάλη γκάμα απειλών κατά της ακεραιότητας του υπολογιστή σας.

ΕΛΕΓΧΟΙ ON-LINE. Εάν δεν υπάρχει εγκατεστημένο στον υπολογιστή σας κάποιο αντι-ιικό ή απλώς θέλετε μια δεύτερη γνώμη, οι παρακάτω διευθύνσεις προσφέρουν δωρεάν ελέγχους on-line του υπολογιστή σας (σε μερικές περιπτώσεις ενδέχεται να καθαρίζουν τους ιούς που εντοπίζουν). Λόγω της χρήσης ActiveX, οι περισσότεροι έλεγχοι on-line απαιτούν τη χρήση του Internet Explorer.

- housecall.trendmicro.com
- security.symantec.com
- support.f-secure.com/enu/home/ols.shtml
- uk.mcafee.com/root/mfs/default.asp
- www.bitdefender.com/scan
- www.kaspersky.com/scanforvirus
- www.pandasoftware.com/products/activescan/com/activescan_principal.htm
- www.ravantivirus.com/scan
- www3.ca.com/securityadvisor/virusinfo/scan.aspx

Παιχνίδια αντικατασκοπίας

Είναι απίστευτος ο αριθμός των παρασιτικών στοιχείων που παραμονεύουν σε κάθε σελίδα Web, ακόμα και σε φαινομενικά αθώες. Η λήψη μέτρων προστασίας είναι κάτι παραπάνω από αναγκαία. Ευτυχώς οι επιλογές αναχαίτισης είναι πολλές και αποτελεσματικές στις περισσότερες των περιπτώσεων.

ΥΠΑΡΧΟΥΝ ΔΕΚΑΔΕΣ ΚΑΤΗΓΟΡΙΕΣ SPYWARE, τα οποία συνήθως βρίσκουν το δρόμο προς τον υπολογιστή μας καθώς σερφάρουμε στο Internet, ειδικά σε «κακόφημους» δικτυακούς τόπους αλλά και μέσω τρίτων εφαρμογών, χωρίς να αφήνουν ίχνος. Στο καταπονητικό γλωσσάριο που παραθέτουμε παρακάτω θα δείτε αναλυτικά κάθε κατηγορία spyware, με τα πλέον σοβαρά να είναι, μεταξύ άλλων, οι dialer, keylogger, τα κατασκοπευτικά cookies αλλά και το ενοχλητικό hijack του Internet Explorer. Σε πρώτο επίπεδο θα προχωρήσουμε σε μια καταγραφή των απειλών κατά της ακεραιότητας του υπολογιστή, έτσι ώστε να σχηματίσουμε την πρώτη γραμμή άμυνας, που δεν είναι άλλη από την όσο το δυνατόν καλύτερη πρόληψη. Δυστυχώς, οι περισσότερες εφαρμογές spyware δεν αφήνουν εμφανή στοιχεία εντοπισμού, με συνέπεια ακόμα και ο έμπειρος χρήστης να είναι δυνατόν να παραπλανηθεί. Σε δεύτερο επίπεδο θα εστιάσουμε σε διάφορα σημάδια τα οποία θα σας βοηθήσουν να καταλάβετε ότι κάτι

δεν πάει καλά στο σύστημά σας, ενώ δεν θα λείψει και μια αναφορά στις εφαρμογές αντιμετώπισης των απειλών spyware. Κατά τη διάρκεια των επικίνδυνων «εξερευνήσεων» που κάνουμε διαπιστώσαμε ότι η πλησιονότητα των εφαρμογών AntiSpyware προσφέρει ικανοποιητικό βαθμό προστασίας σε πολλοπληθή επίπεδα, αλλά ανάλογα με τη μεθοδολογία εντοπισμού που ακολουθούν δείχνουν ευαισθητές προς το A spyware και λιγότερο προς το B.

Οπότε σε πρώτη φάση θα συνιστούσαμε να υπάρχει μια εφαρμογή anti-spyware εγκατεστημένη στο σύστημά σας αλλά θα πρέπει να πραγματοποιούνται τακτικοί έλεγχοι του σκληρού σας δίσκου με τουλάχιστον άλλα δύο διαφορετικά προγράμματα.

ΚΕΡΑΙΖΟΝΤΑΣ ΜΙΑ ΘΕΣΗ ΣΤΟ PC. Οι εφαρμογές AntiSpyware έχουν την ίδια φιλοσοφία με τα αντι-ιικά προγράμματα, ελέγχουν δηλαδή σε πραγματικό χρόνο όλες τις ύποπτες επικοινωνίες

■ Γλωσσάριο κακόβουλων εφαρμογών

SPYWARE. Ο όρος αυτός έχει καθιερωθεί να περιγράφει γενικά όλες τις κακόβουλες ή μη εφαρμογές οι οποίες δημιουργούν διάφορα προβλήματα. Συγκεκριμένα περιγράφουν εφαρμογές που εγκαθίστανται στον υπολογιστή μας αθόρυβα και συλλέγουν πληροφορίες από στοιχεία τηλετρονολογίας έως δικτυακούς τόπους που επισκεπτόμαστε, ρυθμίσεις μητρώου, σύνθεση του υπολογιστή μας κ.ά.

MALWARE. Άλλη μια γενική περιγραφή κακόβουλων εφαρμογών οι οποίες συνήθως περιλαμβάνουν ιούς, δούρειους ίππους και σκουλήκια.

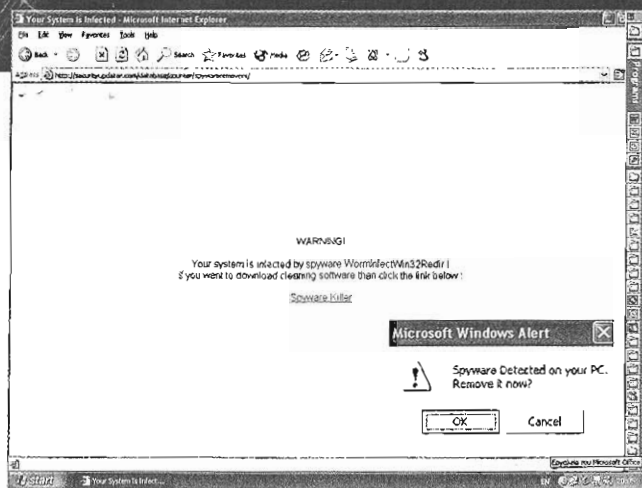
ADWARE. Πρόκειται για λογισμικό το οποίο εισβάλλει στον υπολογιστή μας μέσω κάποιων «δωρεάν» εφαρμογών και προβάλλει διαφημίσεις είτε μέσω της εφαρμογής είτε μέσω του Internet Explorer.

BROWSER HELPER OBJECT. Οι εφαρμογές αυτές έχουν σχεδιαστεί για να επεκτείνουν και να εμπλουτίζουν τον Internet Explorer. Για παράδειγμα, μια ενσωματωμένη στον IE μπάρα

αναζήτησης στο Google κάνει χρήση των BHO. Δυστυχώς τα BHO προσφέρουν μεγάλη ελευθερία κινήσεων και άμεση πρόσβαση στους πόρους του υπολογιστή μας σε κάθε κακόβουλο προγραμματιστή, με συνέπεια να χρησιμοποιούνται για να εμφανίζουν διαφημίσεις, να παραπέμπουν σε άλλους δικτυακούς τόπους κ.λπ.

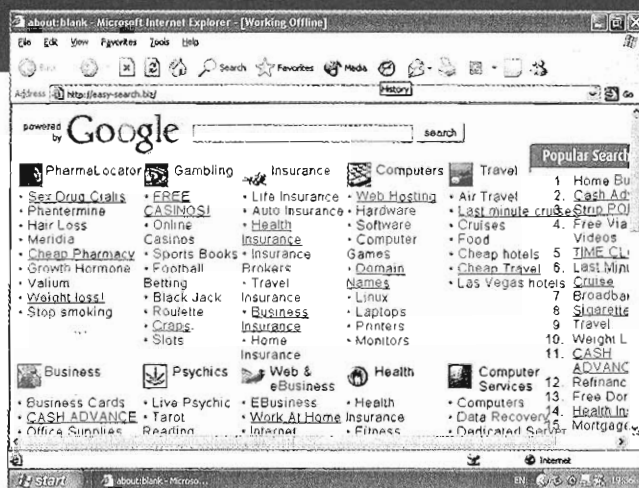
HIJACKER. Άλλη μια ενοχλητική κατηγορία κακόβουλων εφαρμογών οι οποίες εκμεταλλεύονται αδυναμίες του πλοηγού Internet. Αλλάζουν την αρχική σελίδα του πλοηγού και παραπέμπουν σε μια συγκεκριμένη σελίδα αναζήτησης πληροφοριών ή εμφάνισης κάποιου λάθους σύνδεσης. Επίσης είναι δυνατόν να δρομολογούν τις αιτήσεις εμφάνισης σελίδων προς άγνωστους διακομιστές συλλέγοντας με αυτό τον τρόπο πληροφορίες.

KEYLOGGER. Μια ύπουλη κατηγορία κακόβουλων εφαρμογών η οποία καταγράφει σε αρχείο ή αποστέλλει σε συγκεκριμένους παραλήπτες ό,τι πληκτρολογούμε ή ακόμα και όποια ενέργεια εκτελούμε στον υπολογιστή μας, χωρίς την έγκρισή μας



Ο συγκεκριμένος δούρειος ίππος μόλις μόλυνει τον υπολογιστή εμφανίζει ένα παράθυρο μέσω του οποίου πληροφορεί το χρήστη ότι υπάρχει πρόβλημα. Ακολουθώντας παραπέμπει σε ένα δικτυακό τόπο για να «αγοράσει» κάποιο «καθαριστικό». Το πιο πιθανό που μπορεί να συμβεί είναι υποκλοπή του αριθμού της πιστωτικής σας κάρτας.

νώνιες και ενέργειες διαφόρων εφαρμογών στα Windows και προσπαθούν να αποτρέψουν κάθε μόλυνση. Για παράδειγμα, κάθε anti-spyware που σέβεται τον εαυτό του θα πρέπει να ειδοποιεί το χρήστη εάν υλοποιείται κάποια προσθήκη στη λίστα των εφαρμογών που τρέχουν αυτόματα κατά την έναρξη των Windows. Σε αμέσως επόμενο επίπεδο θα πρέπει να έχει τη «νοημοσύνη» να κρίνει το βαθμό επικινδυνότητας της προσθήκης αυτής και είτε να την αποτρέψει είτε να «ρίξει το μπολάκι» στο χρήστη για να αποφασίσει εκείνος. Για παράδειγμα, το Microsoft Antispyware επιτρέπει την εγκατάσταση αρκετών ακίνδυνων εφαρμογών με αυτόματη έναρξη, ενημερώνοντας απλά το χρήστη (με τις αρχικές ρυθμίσεις), ενώ το Spy Sweeper αφήνει την επιλογή σε αυτόν. Βέβαια, στην πρώ-



Ένας γνωστός hijacker του Internet Explorer. Εφόσον μόλυνθείτε, όχι και να κάνετε, η πρώτη σελίδα του πλοηγού θα είναι πάντα μια συγκεκριμένη σελίδα αναζήτησης πληροφοριών.

τη περίπτωση υπάρχει ο κίνδυνος να περάσει κάποια κακόβουλη εφαρμογή, ενώ στη δεύτερη ο χρήστης καλείται να κρίνει την επικινδυνότητα κάθε εφαρμογής χωρίς να έχει αυτή την ικανότητα στις περισσότερες των περιπτώσεων.

ΑΝΤΑΓΟΝΙΣΜΟΣ ΜΕ ΤΑ ANTIVIRUS. Αν και τα anti-spyware ειδικεύονται στην αναζήτηση και την καταστροφή πολλών και διαφόρων κακόβουλων εφαρμογών που τρέχουν χωρίς τη θέλησή μας στον υπολογιστή μας, έχουν επίσης τη δυνατότητα ανίχνευσης πολλών δούρειων ίππων.

Από την άλλη πλευρά οι τελευταίες εκδόσεις των γνωστών AntiVirus μπορούν να εντοπίσουν και να καθαρίσουν πολλά προγράμματα spyware, αφού η συμπεριφορά τους μοιάζει

φυσικά. Όπως καταλαβαίνετε, ο κίνδυνος υποκλοπής αριθμού μιας πιστωτικής κάρτας, για παράδειγμα, είναι μεγάλος.

DIALER. Τα προγράμματα αυτά πραγματοποιούν κλήσεις σε συγκεκριμένους αριθμούς, συνήθως με υψηλή χρέωση, για να επιτρέψουν την πρόσβαση σε συγκεκριμένους δικτυακούς τόπους πορνογραφικού κυρίως περιεχομένου. Μπορούν να διακόψουν μια υπάρχουσα σύνδεση και αθόρυβα να πραγματοποιήσουν νέα σε άλλον αριθμό. Στις περισσότερες περιπτώσεις ο χρήστης πρέπει να κατεβάσει ένα εκτελέσιμο αρχείο και να το τρέξει για να πραγματοποιηθεί η σύνδεση.

ΚΑΚΟΒΟΥΛΑ COOKIE. Τα cookies βοηθούν την αποθήκευση κωδικών πρόσβασης σε δικτυακούς τόπους ή τις επιλογές μας για την εμφάνιση στοιχείων σε ένα δικτυακό τόπο. Κανονικά ο τύπος που επισκεπτόμαστε τα τοποθετεί στον υπολογιστή μας μέσω του πλοηγού Internet. Τα κατασκοπευτικά cookies συλλέγουν πληροφορίες για τους τόπους που επισκεπτόμαστε καθώς και άλλες που δεν θα θέλαμε να μάθει κάποιος. Τα cookies του είδους τα εκμεταλλεύονται συγκεκριμένοι δικτυα-

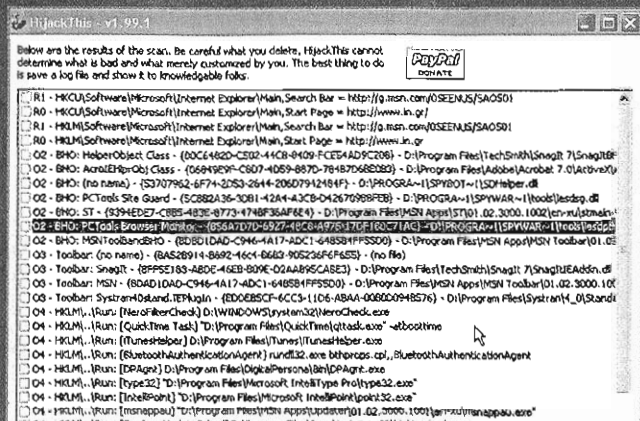
κοί τόποι, συνήθως για διαφημιστικούς ή/και εμπορικούς σκοπούς, αλλά πάντα χωρίς τη συγκατάθεσή μας.

ΑΠΑΤΕΣ E-MAIL (HOAXES). Η συγκεκριμένη κατηγορία e-mail συνήθως περιέχει πληροφορίες για φαινομενικά ενδιαφέροντα θέματα και παρακινεί το χρήστη είτε να επισκεφθεί κάποιο συγκεκριμένο δικτυακό τόπο είτε να προωθήσει το συγκεκριμένο e-mail σε όλη τη λίστα διευθύνσεων που συντηρεί.

ΨΑΡΕΜΑ ΠΛΗΡΟΦΟΡΙΩΝ (PHISHING). Η απάτη συνήθως επιχειρείται μέσω e-mail, με τον αποστολέα να προσποιείται ότι είναι κάποιος σοβαρός οργανισμός, ή, π.χ., μια τράπεζα. Στο e-mail ζητείται από το χρήστη να επισκεφθεί μια συγκεκριμένη σελίδα και να εισαγάγει κωδικούς, αριθμούς πιστωτικών καρτών και διάφορα άλλα προσωπικά στοιχεία. Μεγάλη προσοχή λοιπόν σε e-mail που ζητούν προσωπικά στοιχεία! Το phishing πραγματοποιείται και με άλλους τρόπους, π.χ., με προγράμματα-ρομπότ που ψάχνουν για διευθύνσεις e-mail σε δικτυακούς τόπους. Τα e-mail που ανακαλύπτουν συχνά καταλήγουν στους spammer.

HijackThis

Η εφαρμογή HijackThis (θα τη βρείτε στα CD μας) είναι ένα ισχυρό εργαλείο εξόντωσης διαφόρων απειλών spyware και όχι μόνο. Αυτό που κάνει είναι να εμφανίζει μια λίστα με όλα τα ύποπτα στοιχεία που ζουν στον υπολογιστή σας. Εσείς θα πρέπει να επιλέξετε ποιο από αυτά θα αφαιρεθεί. Σίγουρα απευθύνεται σε έμπειρους χρήστες, οι οποίοι μπορούν να ξεχωρίσουν τα ύποπτα από τα νομότυπα προγράμματα. Οι υπόλογοι χρήστες μπορούν να ζητήσουν τη βοήθεια των εφαρμογών AntiSpyware, οι οποίες ελέγχουν-προτείνουν ενέργειες και διορθώνουν τυχόν προβλήματα με σαφώς πιο αυτοματοποιημένο τρόπο.



Καθαρίζοντας τα παράσιτα

Ad-Aware SE Pro	www.lavasoft.com	30,7€/δωρεάν η έκδοση Personal
Counterspy	www.sunbelt-software.com	15,34€
Mc Afee Anti-Spyware	www.mcafee.com	23€
Microsoft AntiSpyware	www.microsoft.com	δωρεάν, έκδοση Beta
PestPatrol 2005	www.ca.com	23€
Spy Sweeper	www.webroot.com	23€
Spyware Eliminator	www.aluriasoftware.com	23€
Spybot Search and Destroy	www.spybot.info	δωρεάν
SpySubtract Pro	www.internute.com	23€
Spyware Doctor	www.pctools.com	23€

Δεκάδες εφαρμογές κυκλοφορούν με σκοπό τον εντοπισμό και την εξόντωση των πάσης φύσεως παρασιτικών εφαρμογών που ζουν και βασιλεύουν στις κακόφημες και όχι μόνο γειτονιές του Internet. Μέχρι την πραγματοποίηση μιας συγκεκριμένης δοκιμής μεταξύ των εφαρμογών αυτά που θα πρέπει να προσέχετε κατά την επιλογή τους είναι: Η κλήση από όσο το δυνατόν περισσότερα είδη spyware· η συνεχής ενημέρωση των βάσεων δεδομένων για την ανίχνευση των spyware· η δυνατότητα ελέγχου στο υπολογιστικό φόντο όλων των ύποπτων κινήσεων. Στο CD μας θα βρείτε εφαρμογές AntiSpyware σε δοκιμαστική μορφή, οι οποίες επιτρέπουν την ανίχνευση και τον καθαρισμό των παράσιτων για ένα συγκεκριμένο χρονικό διάστημα.

αρκετά με αυτή των ιών και των δούρειων ίππων. Η επικάλυψη αυτή δεν δημιουργεί προβλήματα, αντιθέτως αυξάνει την ασπίδα προστασίας απέναντι σε όλες αυτές τις κακόβουλες εφαρμογές. Περισσότερα για τους δούρειους ίππους, τους ιούς και τα σκουλήκια θα βρείτε στην επόμενη ενότητα.

ΤΟ ΑΝΤΙΤΙΜΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ. Πέρα από το όποιο κόστος κτήσης των εφαρμογών εντοπισμού και καθαρισμού spyware, δεν θα πρέπει να ξεχνάμε το αντίτιμο που πληρώνουμε σε πόρους του συστήματος, με όλες αυτές τις εφαρμογές που είμαστε αναγκασμένοι να τρέχουμε στο προσκήνιο και στο παρασκήνιο. Ο υπολογιστικός χρόνος και η μνήμη είναι οι πιο σημαντικοί πόροι που σπαταλιούνται. Δεν έχουν όλες οι εφαρμογές την ίδια συμπεριφορά, ενώ σε γενικές γραμμές, εφόσον ένα firewall, ένα AntiVirus και ένα AntiSpyware τρέχουν στον υπολογιστή σας, θα λέγαμε ότι τα 512MB RAM είναι απαραίτητα.

ΕΠΙΚΙΝΔΥΝΑ ΜΟΝΟΠΑΤΙΑ. Η ασπίδα που σπλώνουν τα AntiSpyware πάνω από το PC μας είναι μεγάλη και στις περισσότερες των περιπτώσεων αποτελεσματική. Θα λέγαμε ότι υπάρχουν δύο επίπεδα προβλημάτων κατά την πλοήγηση στο Internet. Το πιο ακίνδυνο –χωρίς αυτό να σημαίνει ότι δεν ενοχλεί αρκετό κόσμο– είναι η συλλογή πληροφοριών σχετικά με τις δικτυακές κινήσεις, η οποία οδηγεί στη δημιουργία προφίλ χρήσης για καθέναν από εμάς. Αυτό γίνεται μέσω ειδικών cookies τα οποία στέλνουν στον Internet Explorer ή στον Firefox οι δικτυακοί τόποι που επισκεπτόμαστε.

Εφόσον ο δρόμος σας φέρνει σε τόπους με «ακατόληθλη

για ανηλίκους» περιεχόμενο ή με κωδικούς «σπασίματος» εφαρμογών ή σε δίκτυα Peer to Peer (Kazaa, e-mule κ.λπ.), ανήκετε σίγουρα στην κατηγορία-υψηλού κινδύνου. Πίσω από κάθε κλικ σε αυτούς τους τόπους είναι δυνατόν να κρύβονται διάφορες κακόβουλες εφαρμογές, οι οποίες μπορούν να καταστούν από ενοχλητικές, ανοίγοντας, π.χ., δεκάδες παράθυρα έως και επικίνδυνες εφόσον εγκαταστήσουν κάποιον ιό, δούρειο ίππο ή dialer.

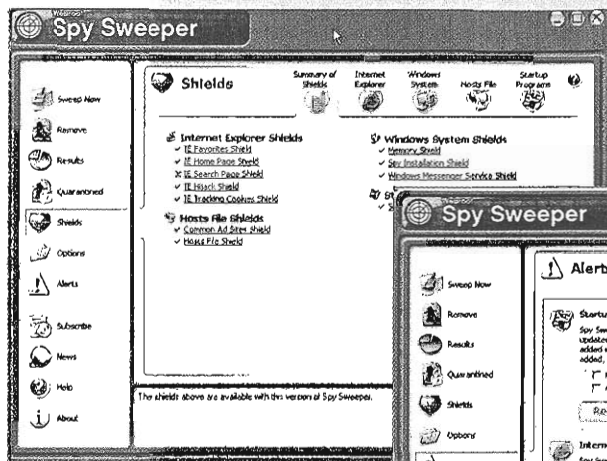
Προγράμματα αναχαίτισης ιών, δούρειων ίππων και spyware θα πρέπει να τρέχουν στο υπόβαθρο του PC σας πάση θυσία. Σε αντίθετη περίπτωση το PC σας θα μεταμορφωθεί σε έναν πλούσιο βιότοπο γεμάτο από κακόβουλο κώδικα, με ό,τι άσχημο συνεπάγεται αυτό για την ασφάλεια του υπολογιστή και των προσωπικών σας στοιχείων.

ΤΑ ΠΡΩΤΑ ΣΗΜΑΔΙΑ. Ανάλογα με το είδος και τον αριθμό των παράσιτων που έχουν μολύνει τον υπολογιστή σας, το πρώτο σημάδι ότι κάτι δεν πάει καλά είναι μια μικρή ή μεγάλη υποβάθμιση της ταχύτητας απόκρισης των Windows έως πτώση ταχύτητας στη σύνδεση με το Internet. Τα πιο συνηθισμένα –σχετικά ακίνδυνα, πλην όμως ενοχλητικά– παράσιτα είναι αυτά που σπάζουν κατά βούληση την αρχική σελίδα του Internet Explorer σε κάποια άλλη διαφημιστική. Στις περισσότερες των περιπτώσεων ο χρήστης δεν μπορεί να επανοφείρει τη σελίδα της απεσκέιας του, ενώ στη χειρότερη περίπτωση σταματά να αποκρίνεται ο Internet Explorer. Το πιο γνωστό Hijack του Internet Explorer είναι το Cool Web Search και οι διάφορες παραλλαγές του.

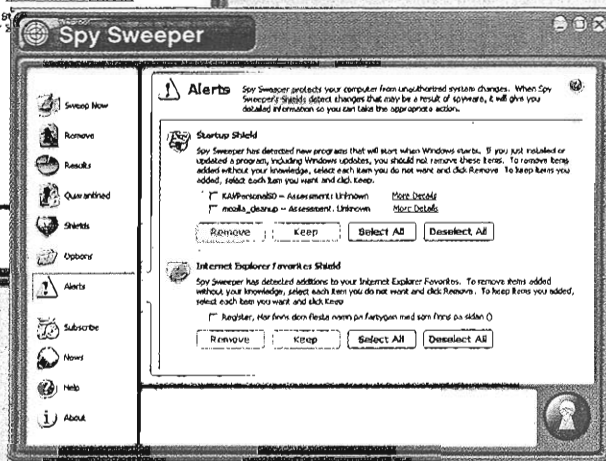
Άλλη μια επικίνδυνη ομάδα παράσιτων είναι αυτά που

■ Spy Sweeper

Το Spy Sweeper της Webroot είναι μια πλήρης και αρκετά γνωστή εφαρμογή προστασίας κατά αρκετών κατηγοριών spyware. Συγκεκριμένα, η τελευταία ενημέρωση ξεπερνά τις 70.000 υπογραφές αναγνώρισης! Μόλις η εταιρεία έχει προσθέσει στη λίστα αρκετές χιλιάδες cookies που κυκλοφορούν στο Internet. Δοκιμαστική έκδοση 30 ημερών, πλήρους λειτουργίας, θα βρείτε στο CD μας.



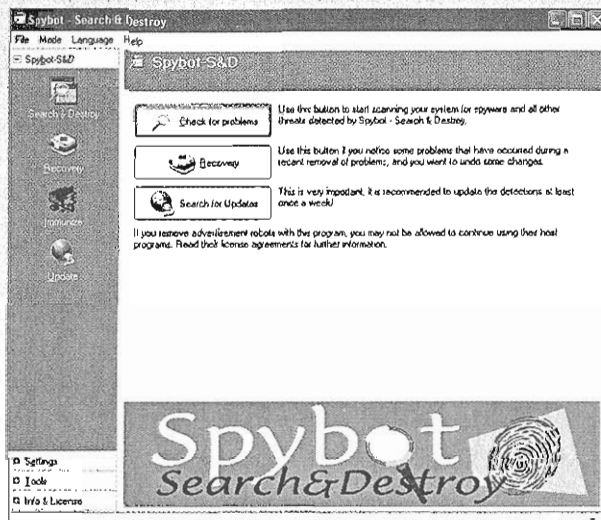
Όλα τα αντι-spyware που σέβονται τον εαυτό τους προσφέρουν προστασία σε πραγματικό χρόνο σε τρία επίπεδα: Ελέγχουν για τυχόν αλλαγές στις ρυθμίσεις του Internet Explorer και αποτρέπουν πιθανό Hijack. Επίσης επιτηρούν τη λίστα εφαρμογών που ξεκινούν αυτόματα μαζί με τα Windows και ενημερώνουν το χρήστη για κάθε αλλαγή/προσθήκη αλλά και για τις ύποπτες κινήσεις και διεργασίες.



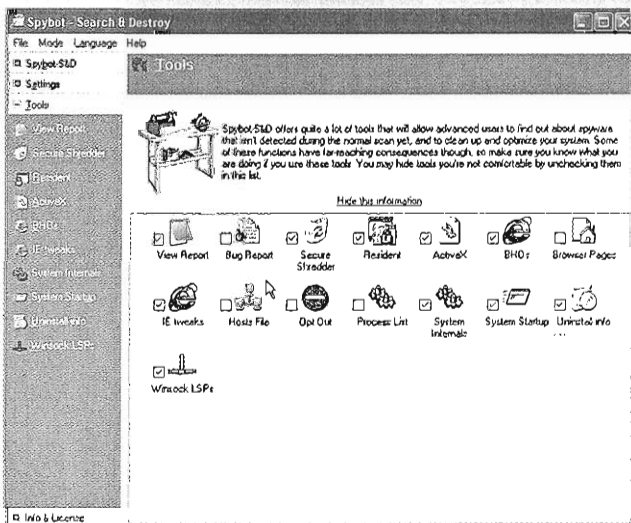
Μόλις εντοπιστεί κάποια αλλαγή στις αγαπημένες διευθύνσεις του Internet Explorer ή στη λίστα των εφαρμογών που τρέχουν μόλις φορτώνουν τα Windows, το Spy Sweeper ζητά τις απαραίτητες επιβεβαιώσεις.

■ Spybot Search & Destroy

Πρόκειται για μια αξιόπαινη δουλειά, αφού οι δημιουργοί της προσφέρουν δωρεάν τη συγκεκριμένη εφαρμογή και τις συνεχείς ενημερώσεις αναγνώρισης spyware. Βέβαια, στο δικτυακό τόπο www.spybot.info παρέχεται η δυνατότητα σε όσους θέλουν να δωρίσουν κάποιο ποσό στους δημιουργούς. Στο CD μας θα βρείτε τη νεότερη έκδοση της εφαρμογής.



Αν και το περιβάλλον εργασίας δεν είναι ακριβώς ο ορισμός της καλαισθησίας, προσφέρει όλα τα απαραίτητα στο χρήστη. Δεν λείπουν οι ενημερώσεις εντοπισμού κακόβουλων εφαρμογών και η δημιουργία αντιγράφων ασφαλείας των αρχείων που επιδιορθώνονται. Ακόμα παρέχεται μόνιμη προστασία στους πλοηγούς Internet Explorer και Opera έναντι επιθέσεων μέσω ActiveX.

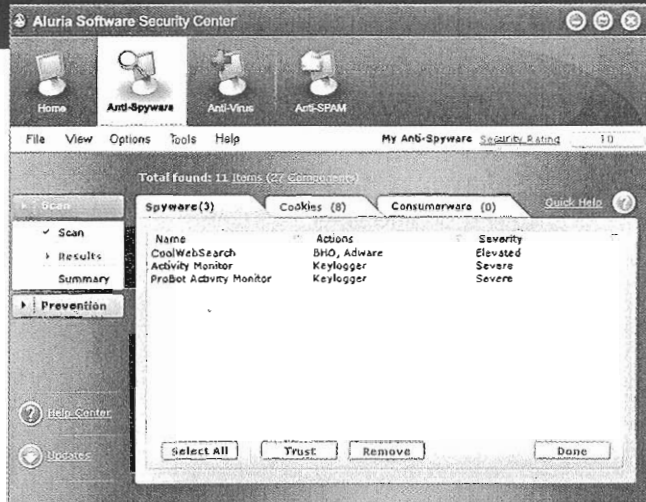


Για τους έμπειρους χρήστες προσφέρονται όλα τα εργαλεία για μη αυτόματο εντοπισμό μιας μεγάλης γκάμας κακόβουλων εφαρμογών.

εκμεταλλεύονται κακόβουλα τις ρουτίνες επέκτασης του Internet Explorer (Browser Helper Object) και το σύστημα ActiveX των Windows. Το ActiveX είναι στην ουσία ένας οργανωμένος τρόπος επικοινωνίας διαφόρων εφαρμογών της Microsoft μεταξύ τους. Μέσω του ActiveX μπορεί να ανοίξει ένα κείμενο του Word μέσα στον Internet Explorer, για παράδειγμα. Σε μια περίπτωση μια κακόβουλη εφαρμογή έβγαζε ένα μικρό παράθυρο, χρησιμοποιώντας το σύστημα ειδοποιήσεων των Windows, το οποίο πληροφορούσε το χρήστη ότι είχε μολυνθεί από κάποιο spyware, και τον παρέπεμπε σε μια σελίδα όπου μπορούσε να αγοράσει (μέσω πιστωτικής κάρτας) εφαρμογές αντι-spyware αμφιβόλου πιστότητας.

ΦΟΥΣΚΩΜΕΝΟΙ ΛΟΓΑΡΙΑΣΜΟΙ ΤΟΥ ΟΤΕ. Δύο από τα πιο ύπουλα και κακόβουλα προγράμματα είναι οι dialer και οι keylogger. Οι dialer, άλλοτε με εμφανή τρόπο και άλλοτε κρυφά, διακόπτουν τη σύνδεση με τον ISP και πραγματοποιούν κλήσεις σε κάποιον αριθμό με υψηλή χρέωση, έτσι ώστε να επιτραπεί η πρόσβαση σε κάποιο δικτυακό τόπο, για παράδειγμα, με πορνογραφικό περιεχόμενο. Εφόσον ο χρήστης δεν καταλάβει εγκαίρως τι συμβαίνει με τη σύνδεσή του, ο επόμενος λογαριασμός του ΟΤΕ θα του επιφυλάσσει μια δυσάρεστη έκπληξη.

Οι Keyloggers εγκαθίστανται αθόρυβα στο σύστημα και χωρίς να αφήνουν ίχνη καταγράφουν ό,τι πληκτρολογήσει ο



Το Spyware Eliminator 4.0 διακρίνεται για την απλότητά του τόσο στον εντοπισμό των κακόβουλων εφαρμογών όσο και στο τρόπο επικοινωνίας με το χρήστη. Στη συγκεκριμένη περίπτωση το σύστημα έχει μολυνθεί με δυο άκρως επικίνδυνους keylogger και το γνωστό CoolWebSearch (CWS). Το CWS είναι μια κακόβουλη εκμετάλλευση των Browser Helper Object του Internet Explorer. Το Spy Sweeper στην έκδοση 3.5 μπορεί να καθαρίσει τις περισσότερες παραλλαγές του CoolWebSearch όπως και το γνωστό μίνι καθαριστικό CWSshredder το οποίο θα βρείτε στο CD μας.

χρήστης ή τους δικτυακούς τόπους που επισκέπτεται. Όλα αυτά τα στοιχεία συνήθως αποθηκεύονται τοπικά, ενώ είναι δυνατόν η εφαρμογή να τα στέλνει σε κάποια συγκεκριμένη διεύθυνση στο Internet ή ακόμα χειρότερα να επιτρέπει σε

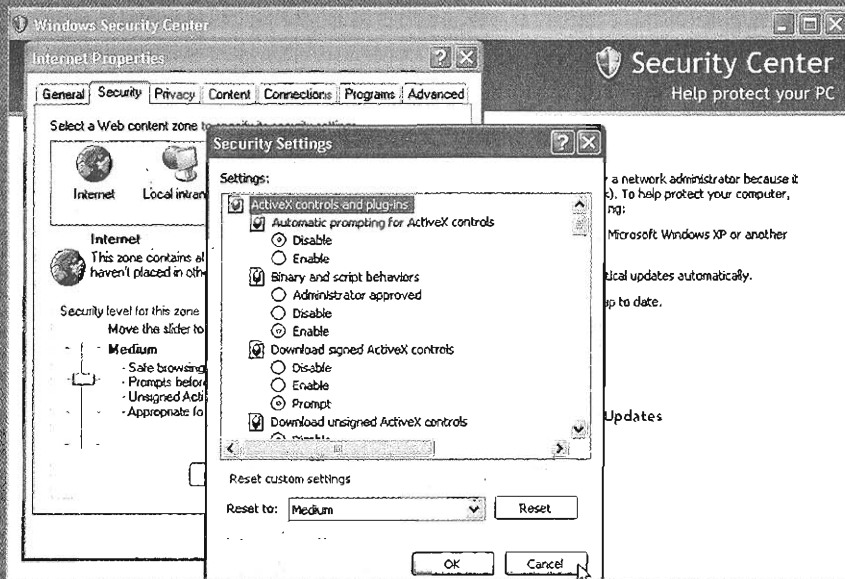
■ Internet Explorer: Ναι ή όχι;

Πολύς λόγος γίνεται σχετικά με τα προβλήματα ασφαλείας των Windows αλλά και του Internet Explorer. Πολλοί είναι αυτοί που έχουν αντικαταστήσει τον IE με τον Firefox ή τον Opera για να μειώσουν τις πιθανότητες μόλυνσεων από κακόβουλες εφαρμογές. Το αδύνατο σημείο του IE δεν είναι άλλο από το σύστημα ActiveX. Έξυχνες και λειτουργικές τεχνολογίες, όπως τα Browser Helper Objects και το ActiveX, έχουν πολλές αδυναμίες, ενώ υπάρχουν πολλοί που τις εκμεταλλεύονται εις βάρος μας.

Από τις ρυθμίσεις ασφαλείας του IE έχετε τη δυνατότητα να περιορίσετε ή να απενεργοποιήσετε το ActiveX, αλλά υπάρχει μεγάλη πιθανότητα να περιορίσετε έτσι και τη λειτουργικότητα των ιστοσελίδων που επισκέπτεστε. Μπορείτε να παίξετε με τις ρυθμίσεις ActiveX και να βρείτε τη χρυσή τομή. Εάν δεν εμπιστεύεστε τον IE, χρησιμοποιήστε τον Mozilla Firefox ή τον Opera, που δεν υποστηρίζουν εντολές ActiveX [ο Opera υποστηρίζει ActiveX με ειδικές προσθήκες τρίτων]. Βέβαια, και πάλι δεν είστε πλήρως εξασφαλισμένοι, αφού πάντα παραμονεύουν οι αδυναμίες της Java και της

Javascript αλλά και αυτές των ίδιων των ενοηλακτικών πλοηγών (βλ. πρόσφατη ενημέρωση ασφαλείας 1.02 του Firefox).

Πάντως, όλα τα σύγχρονα αντι-spyware επιτηρούν και προστατεύουν τον IE σε πολλά επίπεδα, ενώ η Microsoft συνεχώς παρουσιάζει ενημερώσεις ασφαλείας τις οποίες θα πρέπει να εγκαθιστάτε άμεσα. Η επιλογή είναι δική σας.



κάποιον τρίτο να εισέρχεται στον υπολογιστή σας και να παίρνει τα στοιχεία, ανοίγοντας με αυτό τον τρόπο μια κερκόπορτα για διάφορες κακόβουλες ενέργειες.

Οι keylogger είτε αποτελούν μέρος μιας επίσημης σουίτας παρακολούθησης κινήσεων σε υπολογιστές είτε μπορούν να τοποθετηθούν από τρίτους έπειτα από κάποια εγκατάσταση εφαρμογής υψηλού κινδύνου ή μέσω ενός δούρειου ίππου που έχει μόλυνει τον υπολογιστή.

ΒΑΣΙΚΑ ΜΕΤΡΑ. Θα αναφερθούμε σε μερικά μέτρα που θα πρέπει να ληφθούν, έτσι ώστε να περιοριστεί η έκθεση σε πάσης φύσεως κινδύνους από spyware.

1ο μέτρο: Αποφύγετε ή περιορίστε τις επισκέψεις σε δικτυακούς τόπους υψηλού κινδύνου.

2ο μέτρο: Θα πρέπει να εγκαθιστάτε όλες τις κρίσιμες ενημερώσεις των Windows από το Windows Update.

3ο μέτρο: Θα πρέπει να υπάρχουν εγκατεστημένες στον υπολογιστή σας εφαρμογές AntiSpyware και AntiVirus

4ο μέτρο: Θα πρέπει οι εφαρμογές αυτές να είναι ενημερωμένες κυρίως σε επίπεδο αναγνώρισης των απειλών (βάσει δεδομένων εφαρμογών spyware) καθώς και σε επίπεδο προγράμματος (νεότερη έκδοση).

5ο μέτρο: Θα πρέπει να γίνεται τακτικός έλεγχος του σκληρού δίσκου ανά τακτά χρονικά διαστήματα, κατά προτίμηση

από τουλάχιστον δύο ή τρεις διαφορετικές εφαρμογές AntiSpyware ή και με κάποιο AntiVirus το οποίο μπορεί να ανιχνεύσει και να καταστρέψει εφαρμογές spyware.

6ο μέτρο: Εξοικειωθείτε όσο το δυνατόν καλύτερα με τις βασικές λειτουργίες του υπολογιστή σας και των εφαρμογών που τρέχουν κατά την εκκίνηση. Για παράδειγμα, μια γενική μείωση της ταχύτητας απόκρισης των Windows ή της σύνδεσης με το Internet θα πρέπει να σας βάλει σε υποψίες. Επίσης οποιαδήποτε αλλαγή στη συμπεριφορά του μόντεμ θα πρέπει να σημάνει συναγερμό. Ελέγχετε ανά τακτά χρονικά διαστήματα τη λίστα με τις εφαρμογές που έχουν εγκατασταθεί στον υπολογιστή σας. Αρκετά προβλήματα προέρχονται από νομιμοφανή προγράμματα spyware τα οποία μπορούν να απεγκατασταθούν.

ΕΛΕΓΧΟΙ ON-LINE ΓΙΑ SPYWARE. Αρκετοί δικτυακοί τόποι προσφέρουν έλεγχο on-line για spyware. Συνήθως εντονίζουν μόνο το πρόβλημα και σας κατευθύνουν σε κάποια αντίστοιχη εφαρμογή για τον καθαρισμό. Ενδεικτικά παραθέτουμε μερικές διευθύνσεις:

download.zonelabs.com/bin/promotions/spywaredetector/index3.html

www3.ca.com/securityadvisor/pest/pestscan.aspx

www.webroot.com/services/spyaudit_03.htm