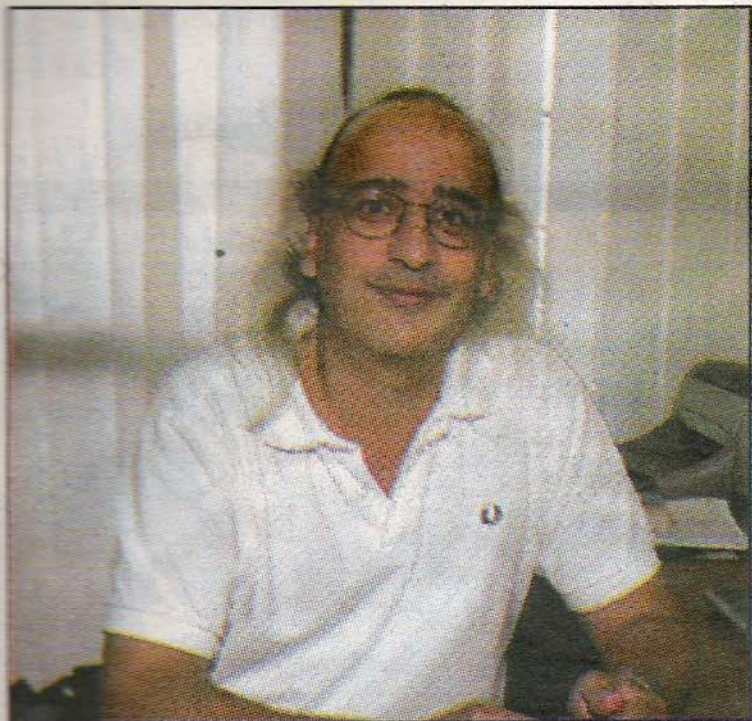


Η ΤΟΛΜΗ

Ηλεκτρονικοί “διαρρήκτες”



Ο καθηγητής της
Επιστήμης των
Ηλεκτρονικών
Υπολογιστών στο ΙΤΕ
Ευάγγελος Μαρκάτος
μίλησε στην “Τ” για τους
«χάκερ», για τα μέτρα
προστασίας που
οφείλουμε να
λαμβάνουμε, τους
τρόπους εισβολής τους
στα συστήματα, αλλά και
για τα ηλεκτρονικά ίχνη
που αφήνουν.

ΣΕΛΙΔΕΣ 12-13

Ηλεκτρονικοί "διαρρήκτες" του Διαδικτύου

Πόσο κινδυνεύουμε από τη

δράση των χάκερ

Τους δικούς τους «διαρρήκτες» έχουν οι υπολογιστές. Υπάρχουν περιπτώσεις ατόμων, που παραβιάζοντας τα συστήματα ασφαλείας, αποδεικνύουν τις ικανότητές τους στους υπολογιστές, αλλά και αυτοί που προχωρούν σε εκβιασμούς εταιριών και φυσικών προσώπων, υποκλέπουν προσωπικά δεδομένα και ωφελούνται οικονομικά, μεταφέροντας μεγάλα χρηματικά ποσά στο λογαριασμό τους. Η δράση των τελευταίων υπάγεται στο λεγόμενο «ηλεκτρονικό έγκλημα».

Ο καθηγητής της Επιστήμης των Ηλεκτρονικών Υπολογιστών στο ΙΤΕ Ευάγγελος Μαρκάτος μίλησε στην "Τ" για τους «χάκερ», για τα μέτρα προστασίας που οφείλουμε να λαμβάνουμε, τους τρόπους εισβολής τους στα συστήματα, αλλά και για τα ηλεκτρονικά ίχνη που αφήνουν.

Τι σημαίνει "χάκινγκ". Ποιος είναι ο "χάκερ";

ΡΕΠΟΡΤΑΖ
Μαρία
Ζαννιά

"Αυτές οι έννοιες έχουν πολλούς ορισμούς. Συνήθως, στην περιοχή των επιστημών της ασφάλειας των υπολογιστών χρησιμοποιείται ο όρος «attacker» που σημαίνει «επιτιθέμενος», αυτός, δηλαδή, που «επιτίθεται» στην ασφάλεια των συστημάτων. Στο ευρύ κοινό βέβαια έχει επικρατήσει ο όρος «χάκερ». Ο «χάκερ» επιτίθεται στο σύστημα μέσω του Διαδικτύου, που συνδέει όλους τους υπολογιστές μεταξύ τους. Αυτός ο όρος παλαιότερα ήταν τιμητικός, υποδήλωνε τον ειδικό στην χρήση των υπολογιστών. Με τα χρόνια έχει αποκτήσει αρνητική έννοια".

Ποιοι κινδυνεύουν;

"Θεωρητικά οποιοσδήποτε έχει έναν υπολογιστή στο Διαδίκτυο μπορεί να αποτελέσει στόχο των «χάκερ». Ωστόσο, υπάρχουν στόχοι υψηλού και χαμηλού κινδύνου. Στόχο υψηλού κινδύνου αποτελούν οι τράπεζες και οι οργανισμοί που έχουν χρήματα, με τους επιτιθέμενους να στοχεύουν στις μεταφορές λογαριασμών. Επίσης, δημοφιλείς στόχοι των «ατάκερ» είναι όσοι συναλλάσσονται και εξαρτώνται από το Διαδίκτυο για τον καθημερινό κύ-

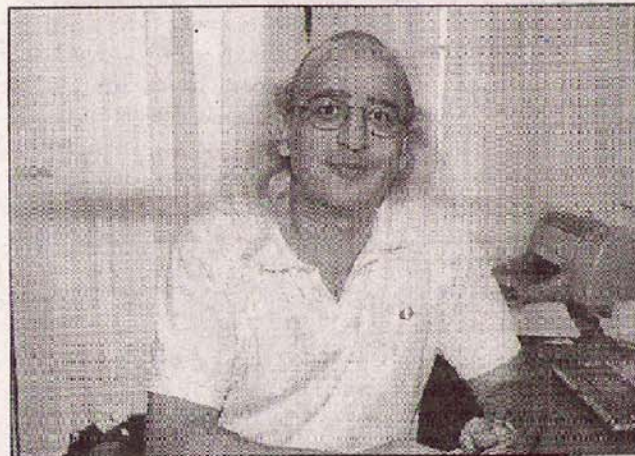
κλο εργασιών τους. Για παράδειγμα, ο επιτιθέμενος μπορεί να εκβιάσει κάποιον που έχει βιβλιοπωλείο στο Διαδίκτυο, απειλώντας να εμποδίσει τη διαδικτυακή πώληση βιβλίων. Τέλος, οποιοσδήποτε υπολογιστής είναι συνδεδεμένος στο Διαδίκτυο μπορεί να αποτελέσει στόχο του «χάκερ», προκειμένου να χρησιμοποιηθεί ως μέσο για να επιτεθεί σε ένα τρίτο υπολογιστή, τον ιδιοκτήτη του οποίου πραγματικά θέλει να εκβιάσει".

Υπάρχουν τρόποι προστασίας; Υπάρχει η απόλυτη προστασία;

"Υπάρχει μια σειρά απλών πραγμάτων που μπορούμε να κάνουμε για να προσφύλαξουμε τους υπολογιστές μας. Οφείλουμε να τους «κλειδώνουμε», όπως ακριβώς πράττουμε για το σπίτι και το αυτοκίνητό μας, να προστατεύουμε τα πιθανά εύαλωτα σημεία τους και να χρησιμοποιούμε προγράμματα τα οποία αποκρούουν ιούς. Επίσης, το λογισμικό που τρέχει στους υπολογιστές πολλές φορές έχει λάθη, τα οποία μπορεί να εκμεταλλευτεί κάποιος επιτιθέμενος, οπότε πρέπει να φροντίζουμε να έχουμε την τελευταία έκδοσή του στον υπολογιστή μας. Απόλυτη προστασία είναι εξαιρετικά δύσκολο να υπάρξει. Σκεφτείτε και τη φυσική ζωή μας. Υπάρχει τρόπος να προστατευόμαστε απόλυτα το σπίτι μας ώστε να μη μπει ποτέ κανείς μέσα; Μπορεί να έχω ένα πολύ καλά θωρακισμένο σπίτι, αλλά ένα παράθυρο μπορεί και να ξεχαστεί ανοικτό".

Με ποιους τρόπους μπορεί να γίνει η "διάρρηξη";

"Ένας τρόπος που χρησιμοποιούν οι επιτιθέμενοι, από τον οποίο είναι δύσκολο να προ-



Ο καθηγητής Ευάγγελος Μαρκάτος.

στατευούμε με τεχνικά μέσα, είναι ο λεγόμενος «σοσιαλ εντζινιερνγκ». Τηλεφωνούν και με ύφος αρκετά σοβαρό - προτιμούν συνήθως νέους υπαλλήλους εταιριών - υποκρίνονται ότι υπάρχει κάποιο πρόβλημα με τον υπολογιστή, ότι αυτοί είναι από το υπολογιστικό κέντρο και ζητούν κωδικούς, προκειμένου να λύσουν το πρόβλημα. Ένας άλλος δημοφιλής τρόπος είναι να στείλουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail), στο οποίο πολλές φορές υπάρχει μια επισυναπτόμενη φωτογραφία ενός δημοφιλούς ηθοποιού ή τραγουδιστή. Φαίνεται, λοιπόν, το μήνυμα να έρχεται από κάποιον γνωστό ή από κάποιον που εμπιστεύεσαι. Από τη στιγμή, όμως, που θα γίνει κλικ στην φωτογραφία, ο επιτιθέμενος έχει τον πλήρη έλεγχο του μηχανήματος του θύματος. Αυτά τα μηνύματα

ονομάζονται «Δούρειο Ίππο».

Ποια προσωπικά δεδομένα μπορούν να υποκλαπεί με αυτό τον τρόπο;

"Αφού μπουν μέσα στο μηχανήμα, μπορούν να κάνουν ένα σωρό πράγματα. Ένα απ' αυτά είναι να εγκαταστήσουν προγράμματα τα οποία καταγράφουν όλα τα πλήκτρα που πατά κάποιος στο πληκτρολόγιο, με αποτέλεσμα να κλέψουν τον κωδικό πρόσβασης μας, τον κωδικό της πιστωτικής μας κάρτας και τον κωδικό του e-mail. Μπορούν να δουν πολλά στοιχεία προσωπικού και οικονομικού χαρακτήρα, πράγμα επικίνδυνο. Η προσωπική μας πληροφορία εκτίθεται προς τα έξω".

Πολλοί ισχυρίζονται ότι οι "χάκερ" δεν είναι τόσο νοήμονες, αλλά ότι απλά εκμεταλλεύονται τις αδυναμίες των συστημάτων.

"Υπάρχουν επιτιθέμενοι οι οποίοι είναι

πολύ έξυπνοι. Μαθαίνουν τις αδυναμίες των συστημάτων και τις εκμεταλλεύονται. Είναι μάλιστα τόσο έξυπνοι, ώστε να αυτοματοποιούν τη διαδικασία, να φτιάχνουν, δηλαδή, προγράμματα τα οποία αυτόματα «χτυπάνε» εκατομμύρια συστήματα, το ένα μετά το άλλο, ωσπου να βρουν τα εύαλωτα. Αυτά τα αυτόματα προγράμματα μπορούν, όμως, να χρησιμοποιηθούν από κάποιον που απλά ξέρει να τα εκτελεί. Με αυτήν την έννοια υπάρχουν οι ευφείς που παράγουν τέτοια συστήματα και αυτοί που έχουν πρόσβαση σε αυτά και μπορούν να επιτεθούν".

Ποιός λόγος γίνεται για τα ηλεκτρονικά ίχνη.

"Αν κάποιος σας πάρει τηλέφωνο στο κινητό σας είναι δυνατό να δείτε, τις περισσότερες φορές, τον αριθμό του. Αυτό είναι ένα ίχνη. Το ίδιο συμβαίνει και με τους υπολογιστές. Είναι πιθανό το θύμα - υπολογιστής να βρει ποιος του επιτίθεται, ανιχνεύοντας την «ιστορική» της εισβολής προς τα πίσω. Βέβαια, τα πράγματα δεν είναι τόσο απλά. Μπορεί να δημιουργηθεί αλυσίδα από ίχνη που να εντοπίζονται σε υπολογιστές διασκορπισμένους σε διαφορετικά μέρη του κόσμου και σε υπολογιστές με πολλούς χρήστες. Έτσι είναι αναγκαία η συνεργασία διαφορετικών αστυνομικών. Οι πολλοί έξυπνοι χάκερ είναι σε εέση να εβήσουν τα ίχνη τους, όμως αν οι ασχέρες συνεργαστούν και αφιερώσουν τον απαραίτητο χρόνο είναι απίθανο να ξεφύγουν".