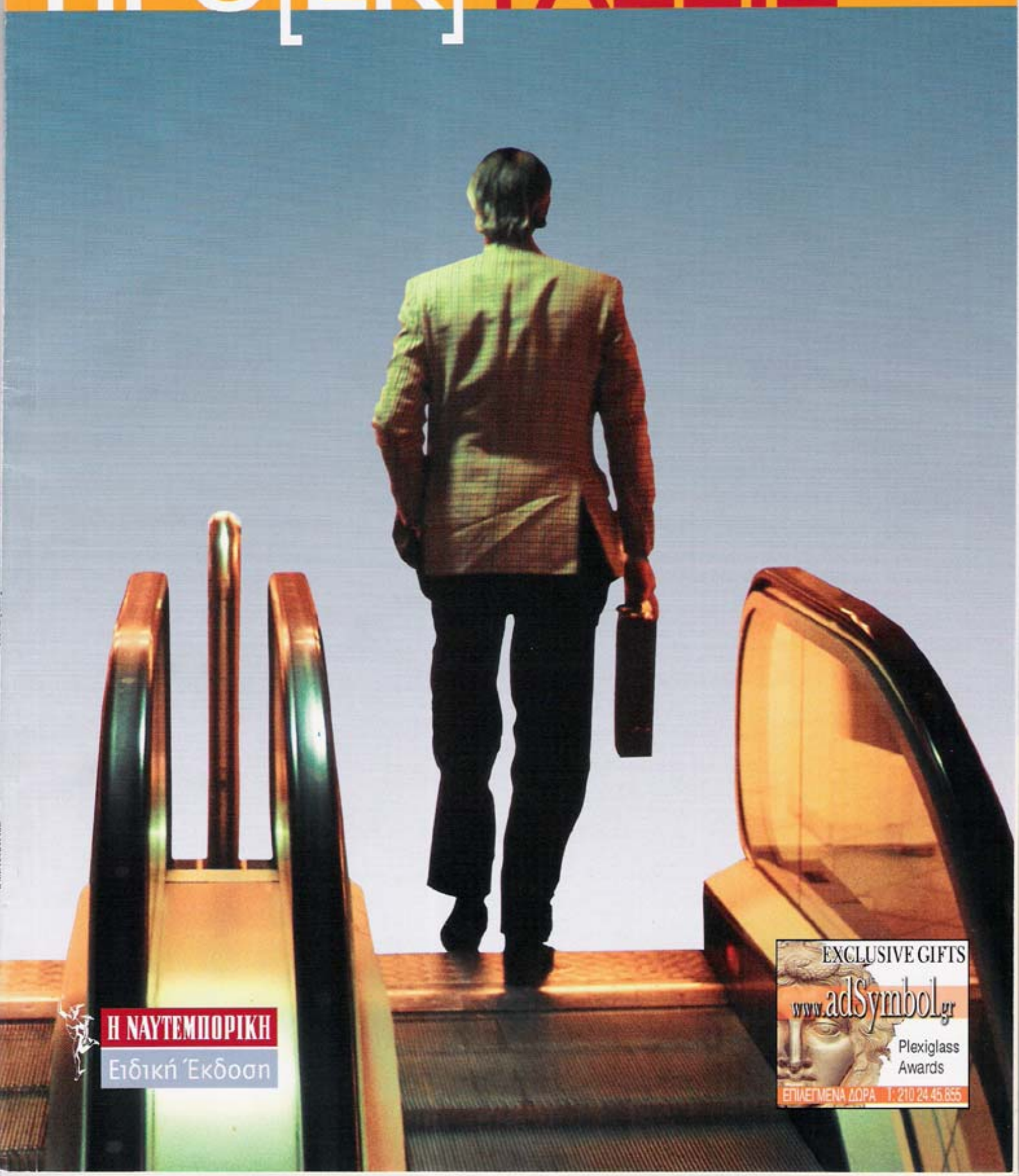
ΕΤΗΣΙΑ ΕΚΔΟΣΗ | ΔΕΚΕΜΒΡΙΟΣ 2006

ΠΡΟ[ΕΚ]ΤΑΣΕΙΣ



Η ΝΑΥΤΕΜΠΟΡΙΚΗ
Ειδική Έκδοση

Υπολογιστής honeypot

Ανακαλύπτοντας τους hackers με δόλωμα ένα «βάζο μέλι»

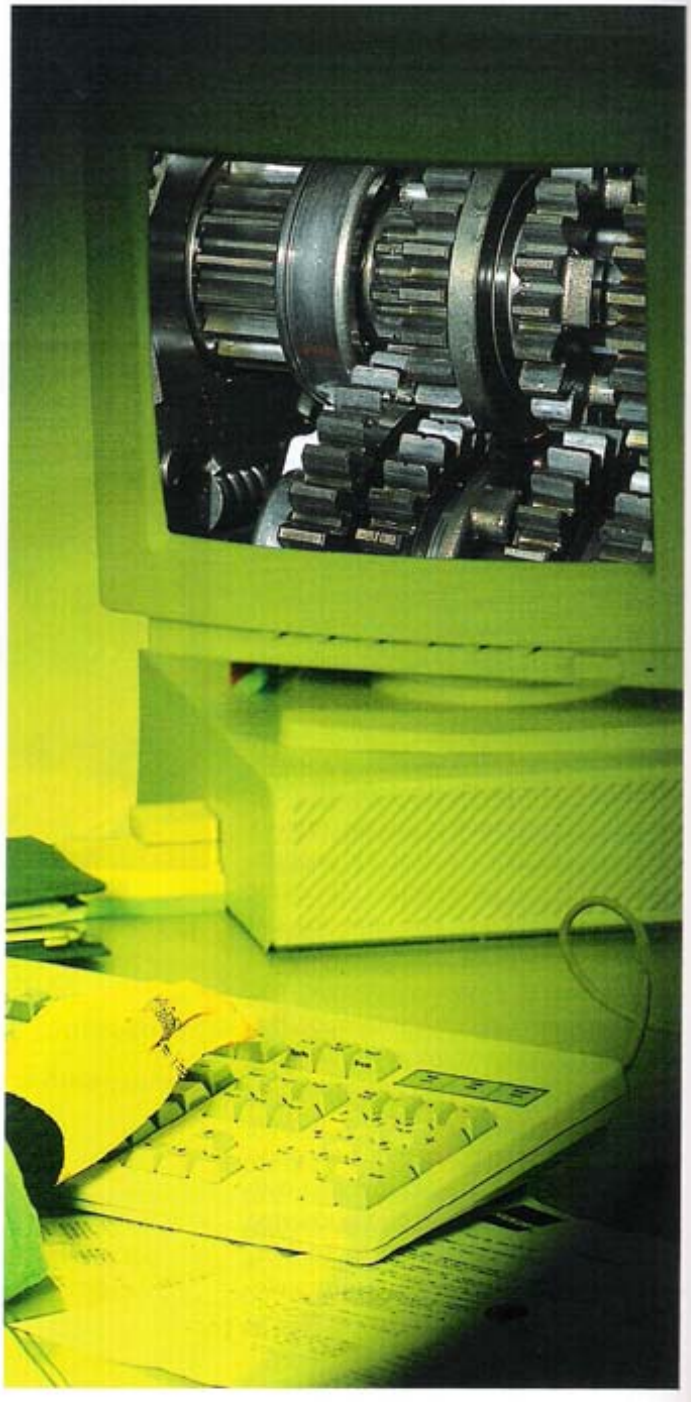
Βαγγέλης Μαρκάτος.

Σπύρος Αντωνάτος.

Κώστας Αναγνωστάκης.

Των **Βαγγέλη Μαρκάτου, Σπύρου Αντωνάτου** και **Κώστα Αναγνωστάκη**,
Ινστιτούτο Πληροφορικής - Ίδρυμα Τεχνολογίας και Έρευνας

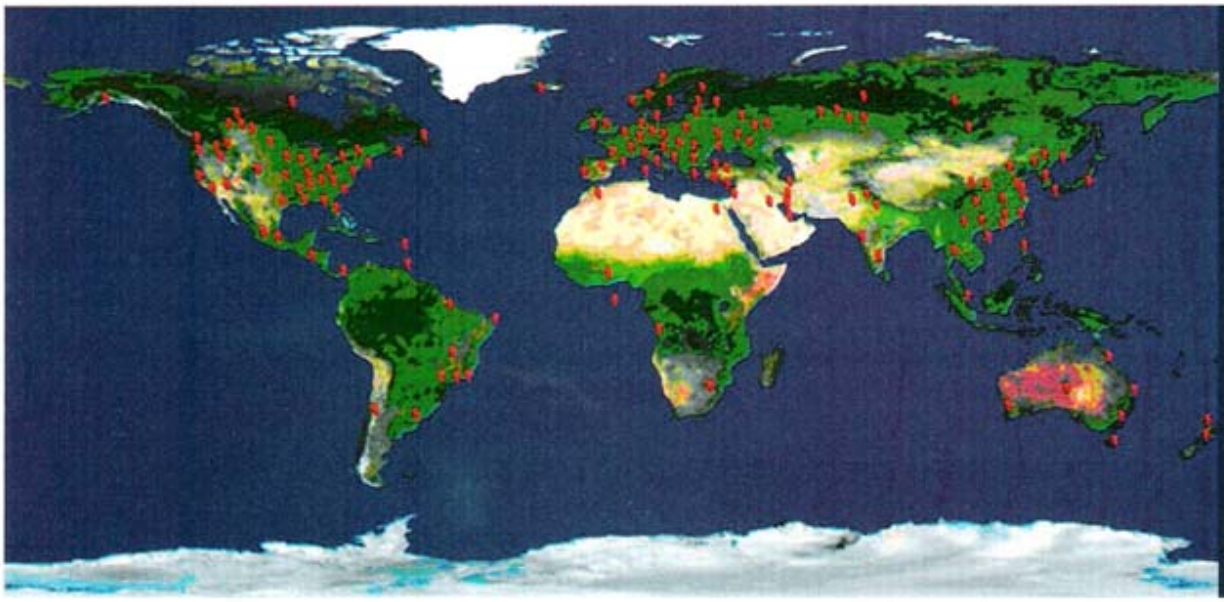
Τα τελευταία χρόνια γινόμαστε μάρτυρες μίας ολοένα και περισσότερο αυξανόμενης επιθετικής δραστηριότητας στο Διαδίκτυο. Πράγματι, οι επιτιθέμενοι του Διαδικτύου, γνωστοί με το όνομα «hackers», εκμεταλλευόμενοι κυρίως αδυναμίες του λογισμικού των υπολογιστών, καταφέρνουν να αποκτήσουν πρόσβαση σε αυτούς τους υπολογιστές, τους οποίους μετά μπορούν να τους χρησιμοποιήσουν για όποιο παράνομο σκοπό θέλουν.



Ορμώμενοι αρχικά από περιέργεια, και σε μεγάλο βαθμό αναζητώντας την κοινωνική αποδοχή μεταξύ των συνεργατών τους, οι hackers έχουν καταφέρει να αποδείξουν ότι μπορούν να κυριεύσουν και να θέσουν υπό τον έλεγχό τους δεκάδες χιλιάδες υπολογιστές μέσα σε λιγότερο από μισή ώρα, χρησιμοποιώντας μία νέα γενιά από αυτο-πολλαπλασιαζόμενα προγράμματα, γνωστά με το όνομα worms (σκουλήκια).

Έχοντας όμως συνειδητοποιήσει την σημασία που έχουν οι τεχνικές τους γνώσεις τους, οι hackers, έχουν αρχίσει τα τελευταία χρόνια να τις εκμεταλλεύονται για οικονομικό όφελος. Έτσι, αντί να προσπαθούν να κυριεύσουν πολλούς υπολογιστές σε μικρό χρονικό διάστημα κάνοντας όσο το δυνατόν περισσότερο θόρυβο γίνεται για να προσελκύσουν όσο το δυνατόν μεγαλύτερη δημοσιότητα και για να

Συνέχεια στη σελίδα 74



Γραφική απεικόνιση των προελεύσεων των επιθέσεων που λάβαμε στα honeypots μας σε διάστημα 2 μηνών.

Συνέχεια από τη σελίδα 72

πετύχουν την κοινωνική καταξίωση στα μάτια των ομοτίμων τους, οι hackers έχουν αρχίσει να εστιάζονται στο πώς θα μπορέσουν να κυριεύσουν υπολογιστές όσο το δυνατόν πιο αθόρυβα γίνεται, χωρίς να γίνουν αντιληπτοί ούτε καν από τον ίδιο τον ιδιοκτήτη του υπολογιστή. Με αυτόν τον τρόπο θέτουν υπό τις διαταγές τους ένα μεγάλο πλήθος υπολογιστών για ένα μεγάλο χρονικό διάστημα, γεγονός που θα τους επιτρέψει να έχουν ένα αξιοσημείωτο οικονομικό όφελος. Αυτοί οι υπολογιστές, οι οποίοι είναι γνωστοί με το όνομα bots (συντομογραφία από το robots), μπορεί να χρησιμοποιηθούν για να στείλουν μηνύματα SPAM, για να κατεβάσουν διαφημίσεις, για να κάνουν επιθέσεις σε τρίτους υπολογιστές, ή απλώς μπορούν να «ενοικιασθούν» σε όποιον ενδιαφέρεται σχετικά (news.bbc.co.uk/1/hi/technology/5407478.stm). Πρόσφατες αποκαλύψεις αναφέρουν ότι hackers κερδίζουν περίπου πέντε χιλιάδες δολάρια το μήνα απλώς νοικιάζοντας τους υπολογιστές που έχουν υπό τον έλεγχό τους.

Προσφέροντας πλήρη ανωνυμία, αυτοί οι υπολογιστές είναι συνήθως το ιδανικό μέσο για την διεξαγωγή παράνομων δοσοληψιών και συναφών δραστηριοτήτων στο Διαδίκτυο.

Στην προσπάθεια καταπολέμησης των hackers στο Διαδίκτυο, ερευνητές από το Ίδρυμα Τεχνολογίας και Έρευνας στο Ηράκλειο Κρήτης αρχικά σχεδίασαν και σήμερα συντονίζουν το ευρωπαϊκό έργο NoAH (A European Network of Affined Honeypots). Για να βρουν και να μελετήσουν τους hackers, οι ερευνητές από το ΙΤΕ χρησιμοποιούν ειδικούς υπολογιστές γνωστούς με το όνομα honeypots (honeypot = βάζο με μέλι). Ένας υπολογιστής honeypot παρουσιάζει, θα λέγαμε, στον hacker ένα εύκολο θύμα και τον «ελκύει», όπως ένα βάζο με μέλι ελκύει τις μέλισσες... Για την ακρίβεια, ο υπολογιστής honeypot περιμένει να του επιτεθεί κάποιος hacker και, όταν δεχθεί επίθεση, καταγράφει όση περισσότερη πληροφορία μπορεί με στόχο να βρει τα εργαλεία που χρησιμοποιεί ο hacker, την αφετηρία του, τις τεχνικές του, και γενικότερα το προφίλ του hacker και της συγκεκριμένης επίθεσης. Αυτό το προφίλ θα το μοιραστεί αργότερα με άλλους υπολογιστές οι οποίοι, βασισμένοι στο προφίλ που θα έχουν στη διάθεσή τους θα μπορούν να αναγνωρίσουν και να αποκρούσουν την ίδια επίθεση ή ακόμα και παρόμοιες επιθέσεις.

Στην προσπάθειά τους να κυριεύσουν όσο το δυνατόν περισσότερους υπολογιστές, οι hackers έχουν αρχίσει να επιτίθενται σε «τυχαίους» υπολογιστές χρησιμοποιώντας μία τεχνική γνωστή με το όνομα «random scanning». Σε αυτή την τεχνική, οι hackers δημιουργούν «τυχαία» ονόματα υπολογιστών με τους οποίους προσπαθούν να επικοινωνήσουν και τους οποίους προσπαθούν να κυριεύσουν. Αν μπορούμε να δώσουμε ένα ανάλογο από την κλασική τηλεφωνία, θα λέγαμε ότι οι hackers πληκτρολογούν εντελώς τυχαία νούμερα στο καντράν του τηλεφώνου ελπίζοντας ότι θα επικοινωνήσουν με κάποιο υπαρκτό τηλέφωνο. Εκμεταλλευόμενο τις τυχαίες αυτές προσεγγίσεις των hackers, το NoAH έχει δημιουργήσει μία υποδομή ώστε να μπορεί να παραλαμβάνει κλήσεις και να απαντά για λογαριασμό υπολογιστών που «δεν υπάρχουν». Δηλαδή αν δει μία επικοινωνία προς έναν υπολογιστή του οποίου το όνομα δεν υπάρχει, ένας από τους υπολογιστές του NoAH αναλαμβάνει προσωρινά την ταυτότητα του ανύπαρκτου υπολογιστή με στόχο να συνομιλήσει με τον hacker και να πάρει όσες περισσότερες πληροφορίες μπορεί για το προφίλ της επίθεσης.

Θέλοντας να δώσει την ευκαιρία και στους απλούς χρήστες των υπολογιστών να βοηθήσουν στην ανίχνευση των hackers, το NoAH έχει δημιουργήσει ένα πρόγραμμα γνωστό με το όνομα «HoneyAtHome». Το HoneyAtHome είναι λογισμικό το οποίο τρέχει σε συνηθισμένους υπολογιστές και προωθεί τις επιθέσεις που δέχονται στους κεντρικούς υπολογιστές του NoAH για περαιτέρω μελέτη και ανάλυση. Απλό στη χρήση του, και αρκετά ελαφρύ στην εκτέλεσή του, το HoneyAtHome μπορεί να τρέξει σε όλα τα δίκτυα, από οικιακά μέχρι και επιχειρήσεων, και προσφέρει χαρακτηριστικά όπως αυτόματα updates, λεπτομερή στατιστικά των επιθέσεων, και διατήρηση της ανωνυμίας του χρήστη.

Βασισμένο λοιπόν στο δέλεαρ των honeypots (των βάζων με το μέλι), στην βοήθεια των απλών χρηστών του HoneyAtHome, και στις προσπάθειες διακεκριμένων ερευνητών, το ευρωπαϊκό έργο NoAH φιλοδοξεί να κάνει ένα σημαντικό βήμα προς ένα ασφαλέστερο Διαδίκτυο για όλους.

Links:

http://dcs.ics.forth.gr/

http://www.fp6-noah.org/

http://www.honeyathome.org

[SID: 2020102]