

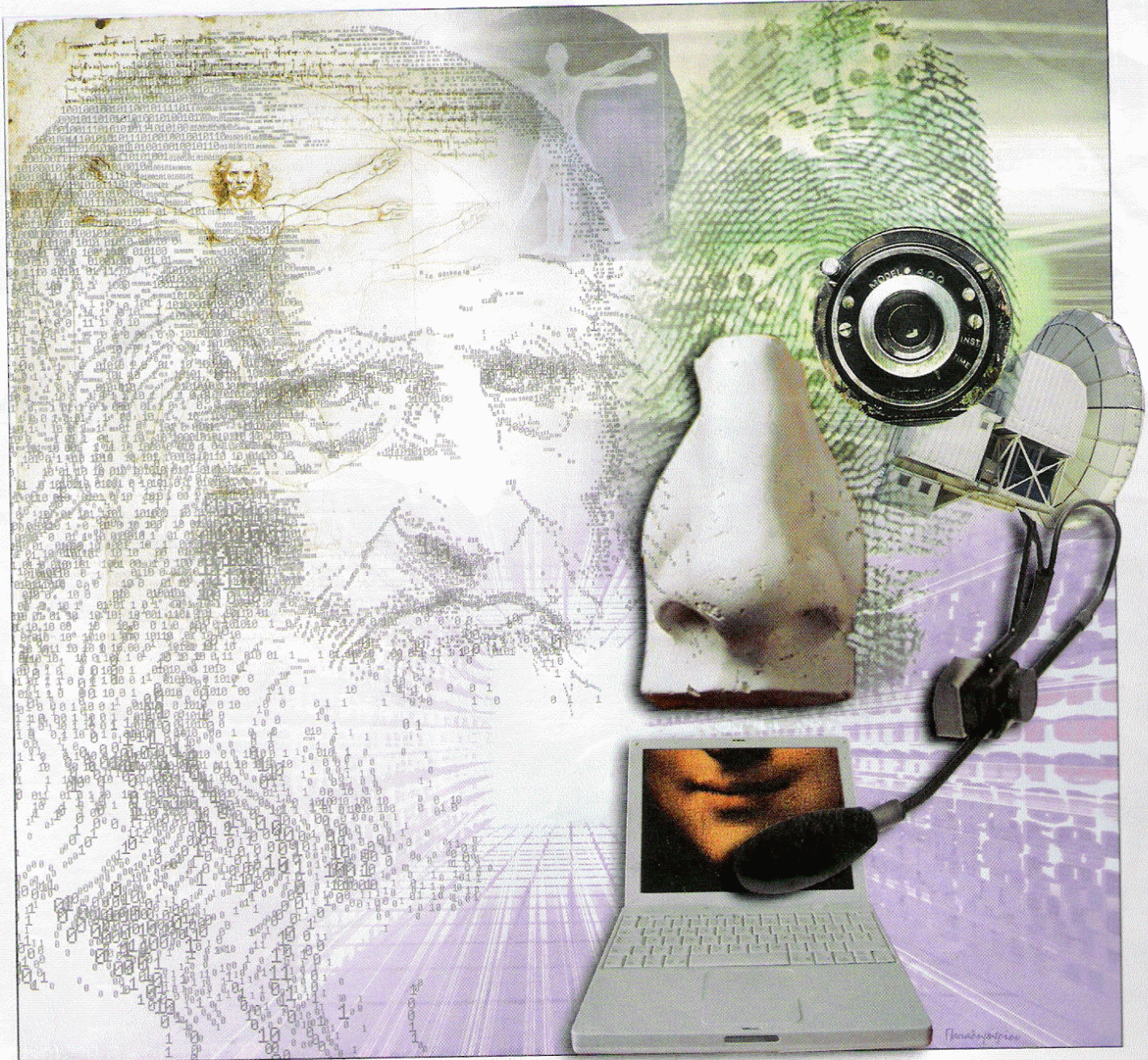


**Αφιέρωμα στη
νεανική επιχειρηματικότητα**

Π. Βουρλούμης: Η μετάλλαξη μιας ΔΕΚΟ
Διάλογος: Ε.Ε & οικονομικός «εθνικισμός»

**The
Economist**

Απρίλιος 2006 τεύχος 27



Η τεχνολογία... των αισθήσεων

Με αφορμή... / Ελληνική άποψη: Ευρυζωνικότητα & δημοτικές εκλογές /
Οι hackers στην καθημερινότητά μας / Οι «ταχύτητες» στην ενέργεια

Μία ευρωπαϊκή πλατφόρμα ανίχνευσης & αναχαίτισης ηλεκτρονικών επιθέσεων στο Διαδίκτυο

Των Σπύρου Αντωνάτου, Κώστα Αναγνωστάκη και Ευάγγελου Μαρκάτου*

Τα τελευταία χρόνια γινόμαστε μάρτυρες ολοένα και περισσότερων ηλεκτρονικών επιθέσεων, οι οποίες, προερχόμενες από κακοπροαίρετους χρήστες και χρησιμοποιώντας ως μέσο μεταφοράς το Διαδίκτυο, έχουν στόχο να διεισδύσουν σε υπολογιστές ανυποψίαστων χρηστών, τόσο στον επαγγελματικό όσο και στον προσωπικό τους χώρο.

Εκμεταλλευόμενες την εξάπλωση της κοινωνίας της Πληροφορίας, την ολοένα και ευρύτερη χρήση εικοσιτετράωρων Διαδικτυακών συνδέσεων τύπου DSL και την ευρεία χρησιμοποίηση εύλωτου, αν όχι διάτρητου, λογισμικού, οι επιθέσεις αυτές τείνουν να γίνουν μια καθημερινό φαινόμενο. Εχοντας, όπως άλλωστε όλοι οι κακοποιοί, πολλά παράξενα ονόματα μεταξύ των οποίων και ιοί (viruses), σκουλήκια (worms) και πίσω πόρτες (back doors), οι ηλεκτρονικές αυτές επιθέσεις, καθώς και τα κακοπροαίρετα προγράμματα που τις συνοδεύουν, εισβάλλουν στην προσωπική μας ζωή, απειλούν την επαγγελματική μας σταθερότητα και θέτουν σε κίνδυνο την ομαλή εξάπλωση της κοινωνίας της πληροφορίας σε πανευρωπαϊκό επίπεδο. Δεν είναι τυχαίο ότι σε πρόσφατη συνέντευξη της η επίτροπος Viviane Reading ανακάλυψε ότι περίπου 50% των Ευρωπαίων πολιτών δεν χρησιμοποιούν ηλεκτρονικές συναλλαγές γιατί ανησυχούν για την ασφάλεια και την προστασία των προσωπικών τους δεδομένων.



λεια και την προστασία των προσωπικών τους δεδομένων.

Αν και έχουν γίνει πολλά βήματα για την ανίχνευση και την καταπολέμηση αυτών των ηλεκτρονικών επιθέσεων, τα περισσότερα από αυτά βασίζονται στην ανθρώπινη παρέμβαση και στην καταλυτική βοήθεια εμπειρογνομόνων, οι οποίοι μόνο αυτοί έχουν τις απαραίτητες γνώσεις να αναγνωρίσουν και να απομονώσουν τέτοιες επιθέσεις. Αυτή η παρέμβαση του ανθρώπινου παράγοντα έχει ως αποτέλεσμα η διαδικασία ανίχνευσης και αναχαίτισης αυτών των ηλεκτρονικών επιθέσεων να είναι αργή, επίπονη και να ολοκληρώνεται πολλές φορές ακόμα και μετά το πέρας της επίθεσης. Πράγματι, πρόσφατες επιθέσεις έχουν αποδείξει ότι μπορούν να κυριεύσουν δεκάδες χιλιάδες υπολογιστές και να περατωθούν μέσα σε λιγότερο από μισή ώρα. Εργαστηριακές μετρήσεις έχουν αποφανθεί ότι προσεκτικά σχεδιασμένες ηλεκτρονικές επιθέσεις μπορούν να κυριεύσουν εκατοντάδες χιλιάδες υπολογιστές μέσα σε λίγα δευτερόλεπτα, μία χρονική κλίμακα η οποία αφήνει ελάχιστα περιθώρια για ανθρώπινη παρέμβαση.

Εχοντας αναγνωρίσει την σημασία και τη σπουδαιότητα αυτού του προβλήματος, το Ινστιτούτο Πληροφορικής στο Ίδρυμα Τεχνολογίας και Έρευνας, έχει σχεδιάσει, έχει ξεκινήσει και είναι σήμερα συντονιστής σε δύο ευρωπαϊκά έργα σχετικά με την ασφάλεια των υπολογιστών στο διαδίκτυο: το LOBSTER και το NoAH, σκοπός των οποίων είναι η δημιουργία της κατάλληλης υποδομής για την έρευνα και την ανάπτυξη καινοτόμων μηχανισμών αντιμετώπισης επιθέσεων στο Διαδίκτυο.

Για την ακρίβεια, το LOBSTER στοχεύει στη δημιουργία πλατφόρμας για επόπτευση

*Ο κ. Ευάγγ. Μαρκάτος είναι καθηγητής του Παν. Κρήτης, στο τμήμα της Επιστήμης των Υπολογιστών και επικεφαλής του εργαστηρίου Παράλληλων και Κατανεμημένων Συστημάτων του ΙΤΕ-ΙΠ. Ο κ.Σ. Αντωνάτος, είναι διδακτορικός μεταπτυχιακός φοιτητής του Παν. Κρήτης και ο κ. Κ. Αναγνωστάκης, είναι συνεργαζόμενος ερευνητής του ΙΤΕ.

Με αφορμή... / Η ελληνική άποψη

89
Απρίλιος 2006

►ση της κίνησης στο διαδίκτυο με σκοπό την αντιμετώπιση προβλημάτων ασφαλείας και απόδοσης. Βασιζόμενο στη διαρκή παρουσία αρκετών σημείων επόπτευσης, και στη μεταξύ τους συνεργασία, το LOBSTER φιλοδοξεί να δημιουργήσει ένα σύστημα έγκαιρης ανίχνευσης και ειδοποίησης ταχύτητα διαδιδόμενων ηλεκτρονικών επιθέσεων. Κύριος σκοπός του LOBSTER είναι η κατασκευή μιας πιλοτικής υποδομής αποτελούμενη από κατανεμημένα σημεία επόπτευσης σε ταχύτητες μεταφοράς δεδομένων από 2,5 έως 10 Gigabits ανά δευτερόλεπτο.

Το τριετές πρόγραμμα NoAH έχει σαν στόχο την ανάπτυξη υποδομής για εντοπισμό επιθέσεων βασισμένο στην τεχνολογία των «honeytraps», δηλαδή υπολογιστών οι οποίοι λειτουργούν σαν «δόλωμα»: οι υπο-

λογιστές honeytraps δεν έχουν κάποια παραγωγική λειτουργία ούτε χρησιμοποιούνται σε τακτική βάση από κάποιο χρήστη, αλλά αντιθέτως τρέχουν εύλωτο λογισμικό με σκοπό να προσελκύσουν κακοπροαίρετους επιτιθέμενους. Αν και δείχνουν εύλωτοι, οι υπολογιστές honeytraps βρίσκονται υπό στενή επόπτευση ώστε να αναλυνονται οι επιθέσεις που δέχονται και να ανιχνεύονται οι πηγές τους. Χρησιμοποιώντας honeytraps γεωγραφικά κατανεμημένα τόσο σε προσωπικούς όσο και σε επαγγελματικούς χώρους το πρόγραμμα NoAH θα σχηματίσει ένα σύστημα έγκαιρης ειδοποίησης το οποίο συσχετίζοντας επιμέρους δεδομένα έχει ως σκοπό την αυτόματη δημιουργία μέτρων αντιμετώπισης ηλεκτρονικών επιθέσεων.

Συμπληρωματικά στην τεχνική προσέ-

γηση, αλλά με κοινό στόχο, τα ευρωπαϊκά έργα LOBSTER και NoAH αποσκοπούν να βοηθήσουν τους παροχείς υπηρεσιών Internet να περιορίσουν τις ζημιές στο δίκτυό τους, να παρέχουν στην ερευνητική κοινότητα μία πληθώρα από δεδομένα για τη βελτίωση των μεθόδων αντιμετώπισης επιθέσεων, να ενδυναμώσουν το συναίσθημα ασφάλειας των πολιτών για το Διαδίκτυο, και να δώσουν την ευκαιρία σε ενδιαφερόμενους οργανισμούς να κατανοήσουν καλύτερα τις πιθανές απειλές τις οποίες εγκυμονεί η ψηφιακή εποχή μας. ▲

Σύνδεσμοι:

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

<http://www.ist-lobster.org>

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

