ΙΟΥΛΙΟΣ - ΑΥΓΟΥΣΤΟΣ 2011
Τεύχος 90

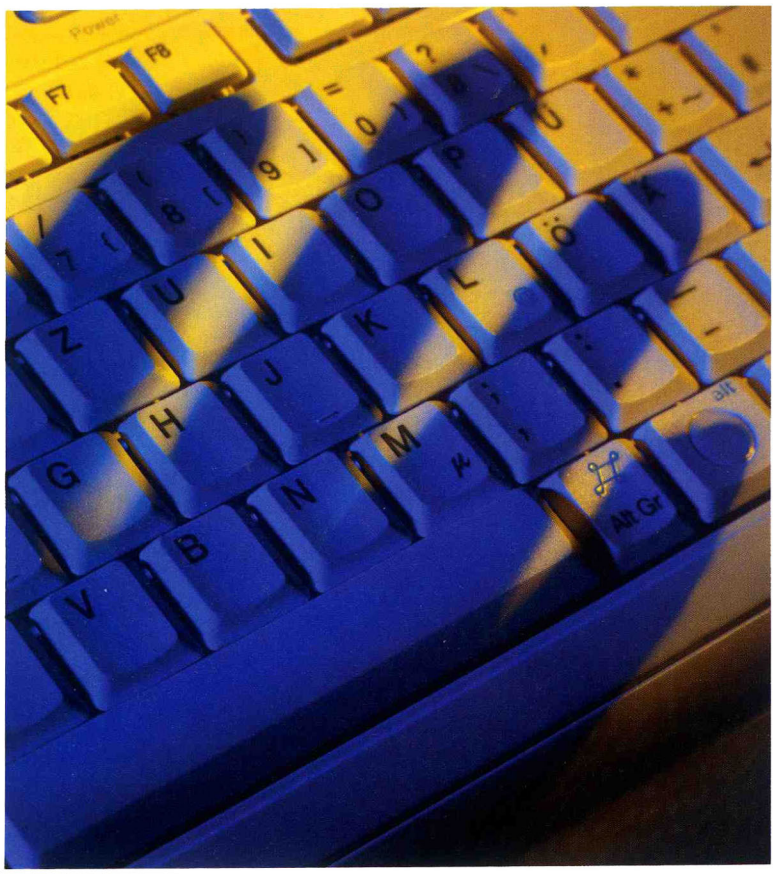
Η ΚΑΘΗΜΕΡΙΝΗ
ΕΙΔΙΚΕΣ ΕΚΔΟΣΕΙΣ

The Economist

Τα tweets της τεχνολογίας

Από το κακόβουλο λογισμικό στα κακόβουλα έγγραφα

ΤΩΝ **ΜΙΧΑΛΗ ΠΟΛΥΧΡΟΝΑΚΗ** ΚΑΙ **ΕΥΑΓΓΕΛΟΥ ΜΑΡΚΑΤΟΥ***



ΤΗΝ ΤΕΛΕΥΤΑΙΑ ΔΕΚΑΕΤΙΑ, η συχνότητα και η πολυπλοκότητα των επιθέσεων που απειλούν τους χρήστες του διαδικτύου αυξάνεται συνεχώς. Αποκτώντας πλήρη πρόσβαση στον υπολογιστή ενός ανυποψίαστου χρήστη, οι κυβερνοεγκληματίες μπορούν να κλέψουν αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης σε διαδικτυακές υπηρεσίες, ή άλλες ευαίσθητες προσωπικές πληροφορίες. Στη συνέχεια, ο μολυσμένος πλέον υπολογιστής μπορεί να χρησιμοποιηθεί για περαιτέρω κακόβουλες ενέργειες, όπως την αποστολή ανεπιθύμητων μηνυμάτων ή την εξάπλωση επιθέσεων προς άλλους υπολογιστές.

Σχεδόν 20 χρόνια μετά την εμφάνισή τους από την εταιρεία Adobe, τα αρχεία τύπου pdf είναι πλέον ο de facto τρόπος διακίνησης ηλεκτρονικών εγγράφων. Εκατομμύρια από τα emails που ανταλλάσσονται καθημερινά περιέχουν συνημμένα αρχεία pdf, ενώ είναι σύνηθες ένα site να προσφέρει μέρος του περιεχομένου του σε μορφή pdf. Μέσω του Adobe Reader, το έγγραφο απεικονίζεται άμεσα στον browser, όπως και μία απλή ιστοσελίδα.

Δυστυχώς, η καθολική αποδοχή των αρχείων pdf, σε συνδυασμό με την αυξημένη πολυπλοκότητα του Adobe Reader λόγω των πλούσιων δυνατοτήτων του, είχε ως αποτέλεσμα την ανακάλυψη μίας σειράς κενών ασφαλείας που οι κυβερνοεγκληματίες δεν άργησαν να εκμεταλλευτούν. Σε αντίθεση με απλούστερους τύπους αρχείων, όπως τα αρχεία εικόνας, ένα αρχείο pdf μπορεί να περιέχει κώδικα, δίνοντας απεριόριστες δυνατότητες στον δημιουργό του, όπως τη συμπερίληψη δυναμικού περιεχομένου και τη δημιουργία αλληλεπιδραστικών εγγράφων. Αντί για κάποια χρήσιμη λειτουργία, ένα κακόβουλο pdf περιέχει κώδικα που εκμεταλλεύεται κάποιο κενό ασφαλείας στο πρόγραμμα απεικόνισης, για να μολύνει τον υπολογιστή.

Δεν είναι η πρώτη φορά που αρχεία εγγράφων χρησιμοποιούνται ως μέσο εισβολής σε υπολογιστές. Το 1999, ο ιός Melissa εξαπλώθηκε ταχύτατα και προκάλεσε υπερφόρτωση σε πολλούς διακομιστές ηλεκτρονικού ταχυδρομείου. Ήταν ένα απλό έγγραφο Microsoft Word με κατάληξη .doc, συνημμένο σε ένα email. Με αντίστοιχο τρόπο, όταν ο παραλήπτης το άνοιγε, ο κακόβουλος κώδικας που περιείχε, μόλυνε τον υπολογιστή και αυτομάτως έστελνε αντίγραφά του σε άλλους χρήστες από την ατζέντα του θύματος.

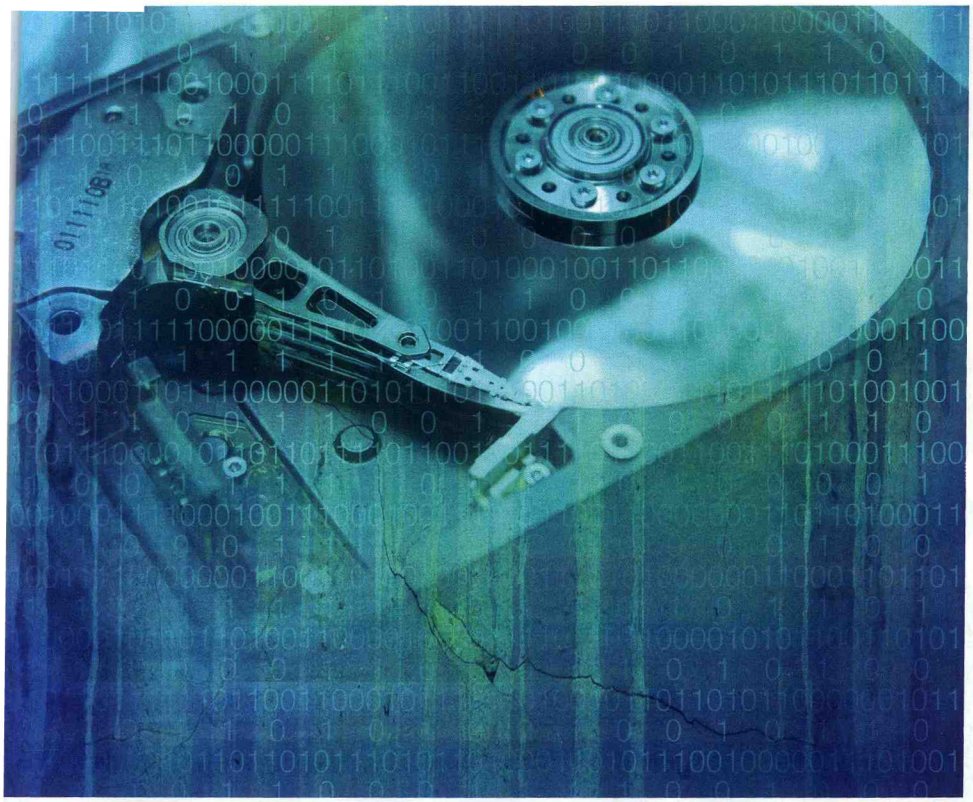
Η αποστολή κακόβουλων pdf μέσω email είναι σημαντικό πρόβλημα, ιδιαίτερα όταν τα μηνύματα είναι αληθοφανή και έχουν στόχο συγκεκριμένους χρήστες. Στα τέλη του 2009, εισβολείς απέκτησαν πρόσβαση σε υπολογιστικά συστήματα της Google μέσω κακόβουλων pdf, συνημμένων σε μηνύματα προς κάποιους από τους υπαλλήλους της εταιρείας. Εκτός από το email, η αυτόματη απεικόνιση αρχείων pdf στον browser με μία απλή επίσκεψη σε μία ιστοσελίδα επιτρέπει την εισβολή στους υπολογιστές χρηστών που απλά έτυχε να επισκεφτούν κάποιο site υπό τον έλεγχο του επιτιθεμένου.

Αυτοί οι δύο μαζικοί τρόποι εισβολής έχουν συμβάλει σημαντικά στη διάδοση της χρήσης κακόβουλων pdf από τους κυβερνοεγκληματίες. Σύμφωνα με μία πρόσφατη μελέτη της Symantec, το ποσοστό των επιθέσεων με χρήση κακόβουλων pdf αυξήθηκε στο 65% το 2010, σε σύγκριση με το 52,6% το 2009.

Οι μεταγενέστερες εκδόσεις του Word διόρθωσαν όλα τα προβλήματα, και πλέον η διακίνηση εγγράφων Word είναι σχετικά ασφαλής. Αντιστοίχα, η νεότερη έκδοση του Adobe Reader έχει σημαντικές βελτιώσεις στον τομέα της ασφάλειας και έως τώρα έχει αποδειχθεί «άτρωτη», ενώ ο Chrome browser διαθέτει πια εγγενή δυνατότητα απεικόνισης pdf αρχείων, χωρίς να απαιτείται εγκατάσταση του Adobe Reader.

Η πλειονότητα, όμως, των υπολογιστών που είναι συνδεδεμένοι στο διαδίκτυο δεν διαθέτει τις τελευταίες ενημερωμένες εκδόσεις όλων των εγκα-

*Ο κ. **Μιχάλης Πολυχρονάκης** είναι μεταδιδακτορικός ερευνητής στο Columbia University.
Ο κ. **Ευάγγελος Μαρκάτος** είναι επικεφαλής του Εργαστηρίου Κατανεμημένων Υπολογιστικών Συστημάτων του Ινστιτούτου Πληροφορικής του ITE, και καθηγητής του Τμήματος Επιστήμης Υπολογιστών στο Πανεπιστήμιο Κρήτης.



τεστημένων εφαρμογών, και ένα μόνο κενό ασφαλείας σε κάποια από αυτές είναι αρκετό για μία επιτυχημένη εισβολή. Επιπρόσθετα μέτρα προστασίας, όπως προγράμματα antivirus και συστήματα ανίχνευσης επιθέσεων, αυξάνουν σημαντικά την ασφάλειά μας στο διαδίκτυο, αλλά δεν είναι πάντα αποτελεσματικά.

Ο τομέας της ανίχνευσης και αντιμετώπισης διαδικτυακών επιθέσεων απασχολεί χιλιάδες ερευνητές σε πανεπιστήμια, ερευνητικά κέντρα και εταιρείες, ενώ οι τελευταίες εξελίξεις παρουσιάζονται σε δεκάδες διεθνή συνέδρια κάθε χρόνο. Τα τελευταία χρόνια, η ερευνητική ομάδα του Εργαστηρίου Κατανεμημένων Υπολογιστικών Συστημάτων στο Ινστιτούτο Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας στην Κρήτη (*http://www.ics.forth.gr/dcs/*) έχει αναπτύξει πρωτοποριακές τεχνολογίες αντιμετώπισης και ανάλυσης κακόβουλου λογισμικού και διαδικτυακών επιθέσεων. Πρόσφατα, στο πλαίσιο του ευρωπαϊκού έργου i-Code (*http://www.icode-project.eu/*), ένα σημαντικό μέρος της έρευνας έχει εστιάσει στην ανίχνευση κακόβουλων εγγράφων pdf και άλλων εξελιγμένων μορφών κακόβουλου κώδικα, και ήδη έχει αποδώσει σημαντικά ερευνητικά αποτελέσματα.

Το οικονομικό κίνητρο των κυβερνοεγκλημάτιών και ο αυξανόμενος αριθμός των υποψήφιων θυμάτων, λόγω του πολλαπλασιασμού των χρηστών του διαδικτύου και της εντονότερης ενασχόλησής μας με τον κυβερνοχώρο, δεν αφήνουν περιθώρια ελπίδας για πλήρη εξάλειψη του κινδύνου. Αν και τα επίπεδα ασφαλείας των διαδικτυακών εφαρμογών έχουν βελτιωθεί σημαντικά, ο ανθρώπινος παράγοντας είναι πάντα κρίσιμος και όλοι μας μπορούμε από απροσεξία να κάνουμε κάποιο σφάλμα. Απλά χρειάζεται να αντιμετωπίζουμε τις συναναστροφές και τις ενέργειές μας στον κυβερνοχώρο με την ίδια περίσκεψη, όπως και έξω από αυτόν. □