

KASPERSKY LAB

## Ασφάλεια στον Κυβερνοχώρο



Οι χρήστες μπορεί να έρθουν αντιμέτωποι με απειλές στις πιο αναπάντεχες και φαινομενικά ασφαλείς τοποθεσίες. Έτσι, κακόβουλοι κώδικες εγκαθίστανται στους υπολογιστές όσων επισκέπτονται την προσβεβλημένη ιστοσελίδα

**Α**κόμα και οι πιο προσεκτικοί χρήστες ηλεκτρονικών υπολογιστών δεν είναι ασφαλείς από ιούς, αν δεν προστατεύονται από κάποια λύση ασφαλείας. Χωρίς να το γνωρίζουν οι χρήστες, οι κυβερνοεγκληματίες εκμεταλλεύονται προσβεβλημένους υπολογιστές για δικό τους όφελος και οι χρήστες αυτοί γίνονται ανυποψίαστοι συνεργοί σε παράνομες δραστηριότητες. Όταν πρόκειται για κακόβουλα προγράμματα, η προειδοποίηση δεν συνεπάγεται προστασία, υποστηρίζουν οι ειδικοί της Kaspersky Lab, οι οποίοι εντοπίζουν 8.000 -10.000 (!) νέους κακόβουλους κώδικες καθημερινά.

Επιπλέον, οι σύγχρονες τεχνικές εξάπλωσης που χρησιμοποιούνται από τους συντάκτες κακόβουλων κωδικών επιτρέ-

πουν τη μόλυνση των υπολογιστών εν αγνοία των χρηστών τους. Οι περισσότεροι δεν αντιλαμβάνονται τον υψηλό κίνδυνο που αντιμετωπίζει ένας "απροστάτευτος" υπολογιστής, όταν ακολουθούνται σύνδεσμοι που οδηγούν σε "αμφισβητήσιμο" υλικό και αποστέλλονται μέσω μηνυμάτων spam ή όταν ανοίγουμε κάποιο συνημμένο αρχείο από άγνωστο αποστολέα. Στην πραγματικότητα το να αποφεύγονται αυτές οι πρακτικές αποτελεί βασικό κανόνα της "ψηφιακής υγιεινής". Παρόλα αυτά, στο πλαίσιο του σύγχρονου κυβερνοχώρου, απλά το να ακολουθεί κανείς αυτούς τους κανόνες δεν επαρκεί.

### Καθημερινοί κίνδυνοι

Σε μια συνέντευξη, ο Eugene Kaspersky ρωτήθηκε αν είναι δυνατόν να διασφα-

λίσουμε έναν υπολογιστή χωρίς λύση ασφαλείας, ακολουθώντας απλά κάποιους βασικούς κανόνες προληπτικής προστασίας. Απάντησε: "Κάποιος μπορεί να θεωρεί έναν υπολογιστή προστατευμένο, πρώτον όταν όλες οι εξωτερικές μονάδες που χρησιμοποιούνται για μεταφορά πληροφοριών (Internet, flash drives, CD/ DVDs) έχουν απενεργοποιηθεί, δεύτερον όταν είναι κλειστός ο υπολογιστής και τρίτον... όταν ο χρήστης κοιμάται. Με άλλα λόγια, είναι αδύνατον να εξασφαλίσετε 100% προστασία από κακόβουλο λογισμικό, ακριβώς όπως είναι ανέφικτο να προστατευτείτε πλήρως από το να κολλήσετε τον ιό της γρίπης".

Σύμφωνα με τον Alex Gostev, Επικεφαλής της Παγκόσμιας Ομάδας Έρευνας και

Ανάλυσης του Kaspersky Lab, “οι σύγχρονοι ιοί προσπαθούν να είναι όσο το δυνατόν πιο ασαφείς, αφού στις περισσότερες περιπτώσεις στοχεύουν στην απόσπαση των προσωπικών σας δεδομένων, διευθύνσεων e-mail και κωδικών πρόσβασης. Χωρίς ειδικό λογισμικό, ο απλός χρήστης δεν θα καταλάβει ποτέ ότι κάτι δεν πάει καλά με τον υπολογιστή του. Ένα πρόγραμμα anti-virus είναι η μοναδική λύση”.

Οι χρήστες μπορεί να έρθουν αντιμέτωποι με απειλές στις πιο αναπάντεχες και φαινομενικά ασφαλείς τοποθεσίες. Επισκέπτεται ο χρήστης την αγαπημένη του ιστοσελίδα καθημερινά ή κάποια δημοφιλή και νόμιμη τοποθεσία με υψηλή επισκεψιμότητα και μόλυνεται ο υπολογιστής γιατί οι hackers έχουν εισβάλει στο συγκεκριμένο ιστότοπο. Έτσι, κακόβουλο κώδικες εγκαθίστανται στους υπολογιστές όσων επισκέπτονται την προσβεβλημένη ιστοσελίδα. Θα πατήσει κάποιος χρήστης ένα σύνδεσμο που υποτίθεται ότι εστάλη από τον “κολλητό” του, για να δει κάποιο διασκεδαστικό βίντεο, μια ενδιαφέρουσα φωτογραφία ή οποιοδήποτε άλλο υλικό και δεν θα

προσέξει ότι ένα Trojan έχει εγκατασταθεί στον υπολογιστή του.

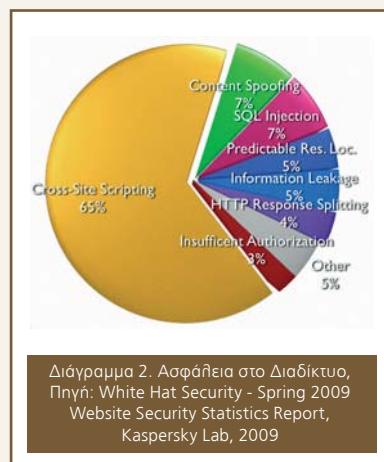
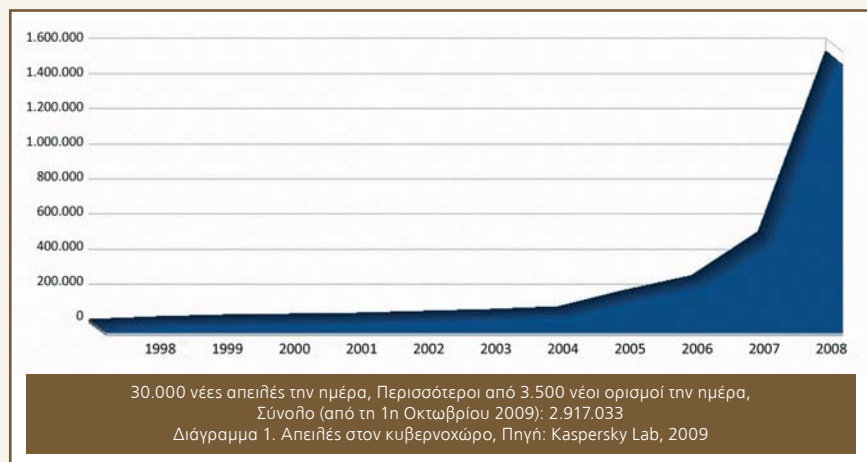
### Κυβερνοέγκλημα

Μόνο κάποια κακόβουλα προγράμματα αποκαλύπτουν την παρουσία τους και μπλοκάρουν τις λειτουργίες του υπολογιστή. Αν ένα μήνυμα εμφανιστεί ως αποτέλεσμα της εισβολής του ιού, κατά πάσα πιθανότητα θα προέρχεται από κάποιον ανώνυμο αποστολέα που θα ζητάει ανταλλάγματα για την αποκατάσταση των πληροφοριών. Οι κυβερνοεγκληματίες του σήμερα δημιουργούν και διαδίδουν κακόβουλο λογισμικό όχι για να γίνουν διαβόητοι, αλλά για να αποκομίσουν κέρδος. Αυτό το καταφέρνουν με το να εκμεταλλεύονται τους υπολογιστές άλλων χρηστών, αφού έχουν αποκτήσει τον έλεγχο τους μετά την εισβολή των ιών.

Οι εγκληματίες αναζητούν την εκμετάλλευση μολυσμένων υπολογιστών, ώστε να εξυπηρετήσουν τα δικά τους συμφέροντα, για όσο μπορούν περισσότερο. Επί της ουσίας, οι εγκληματίες λειτουργούν σαν ένα είδος διαδικτυακού παράσιτου και προσπαθούν να διατηρούν τους κακόβουλους κώδικες σε λειτουργία,

χωρίς να επηρεάζουν την κανονική λειτουργία των μολυσμένων υπολογιστών, ώστε οι χρήστες να μην εντοπίσουν το κακόβουλο πρόγραμμα και να μην το αντιμετωπίσουν αναλόγως. Αν οι εγκληματίες αποκτήσουν πρόσβαση στον υπολογιστή, θα χρησιμοποιήσουν αυτά τα μέσα για το προσωπικό τους συμφέρον, κάνοντας τον χρήστη του υπολογιστή συνεργό στις εγκληματικές τους δραστηριότητες. Αν ο υπολογιστής κάποιου χρήστη έχει ήδη προσβληθεί, δεν αποτελεί παρηγοριά ότι το ίδιο έχει συμβεί σε εκατομμύρια υπολογιστές σε όλο τον κόσμο. Εκατομμύρια προσβεβλημένων υπολογιστών “δουλεύουν” για τους κυβερνοεγκληματίες. Εκατομμύρια χρηστών γίνονται άθελα τους συνεργοί σε κυβερνοεγκλήματα.

Οι εγκληματίες ενώνουν τους προσβεβλημένους υπολογιστές σε δίκτυα, φτιάχνοντας τα λεγόμενα zombie networks, ή botnets. Αυτά τα botnets (υπολογιστές προσβεβλημένοι από κακόβουλο λογισμικό) επιτρέπουν την κινήτη και - κατά κανόνα - κεντρική διαχείριση όλων των υπολογιστών που ανήκουν στο δίκτυο. Συνεπώς, πολλοί υπολογισ-



K A S P E R S K Y L A B

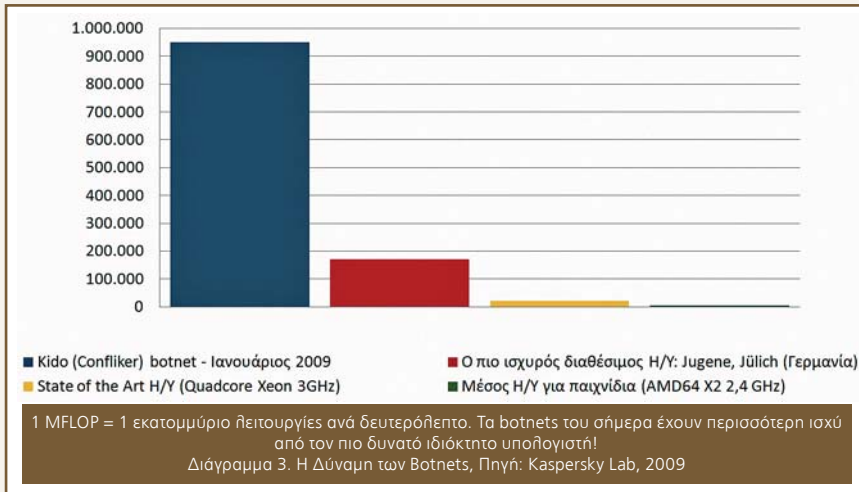
## Ασφάλεια στον Κυβερνοχώρο

Οι κυβερνοεγκληματίες του σήμερα δημιουργούν και διαδίδουν κακόβουλο λογισμικό όχι για να γίνουν διαβόητοι, αλλά για να αποκομίσουν κέρδος.

Αυτό το καταφέρνουν με το να εκμεταλλεύονται τους υπολογιστές άλλων χρηστών, αφού έχουν αποκτήσει τον έλεγχο τους μετά την εισβολή των ιών

στές λαμβάνουν και εκτελούν υπάκουα την ίδια εντολή, την οποία οι ιδιοκτήτες τους δεν γνωρίζουν. Τα σχετικά μικρά zombie networks, τα οποία αποτελούνται από αρκετές χιλιάδες υπολογιστές, είναι αυτά που συναντώνται με μεγαλύτερη συχνότητα στο Διαδίκτυο. Ωστόσο, στο κυβερνοέγκλημα χρησιμοποιούνται και μεγάλου μεγέθους botnets, τα οποία αποτελούνται από 500.000 έως και αρκετά εκατομμύρια υπολογιστές. Έτσι, οι ειδικοί πιστεύουν ότι το Kido, ένα ιδιαίτερα επικίνδυνο κακόβουλο πρόγραμμα, μπορεί να έχει προσβάλει έως και πέντε εκατομμύρια υπολογιστές κατά τη διάρκεια μιας "επιδημίας", στο ξεκίνημα του 2009. Όλοι αυτοί οι υπολογιστές





μετατράπηκαν σε υπάκουα εργαλεία των zombie networks και η διαχείριση τους πέρασε στα χέρια των εισβολέων.

### Ασφάλεια στο Διαδίκτυο - Στατιστικά Στοιχεία

- Το 82% των ιστοσελίδων έχουν κάποιο πρόβλημα σημαντικό, επείγον ή κριτικής σημασίας
  - Μέσος όρος σοβαρών τρωτών σημείων σε ιστοσελίδες που δεν έχουν αντιμετωπιστεί: 7
  - Μέσος όρος επιθέσεων (attack surface) ανά ιστοσελίδα: 227
  - Μέσο όρος του ποσοστού τρωτών σημείων: 2.58%
- Πηγή: <http://www.whitehatsec.com/home/resource/stats.html>

### Συμβουλές

Για να αποφύγετε να γίνετε συνεργοί σε κυβερνοεγκλήματα, μπορείτε να ακολουθήσετε τις συμβουλές των ειδικών στην ασφάλεια των υπολογιστών:

- Χρησιμοποιείστε ολοκληρωμένη τεχνολογία ασφαλείας, συμπεριλαμβανομένων λύσεων antivirus και firewall.
- Εγκαταστήστε μόνο αδειοδοτημένο λογισμικό. Το πρόβλημα με το πει-

ρατικό λογισμικό δεν περιορίζεται απλά στην καταπάτηση πνευματικών δικαιωμάτων. Οι ιστοσελίδες με πειρατικό λογισμικό μπορεί να περιέχουν κακόβουλο λογισμικό που μοιράζει με δωρεάν λογισμικό.

- Το νόμιμο λογισμικό ενημερώνεται σε τακτική βάση. Δώστε σημασία στις ενημερώσεις του λογισμικού που χρησιμοποιείτε στον υπολογιστή σας και εγκαταστήστε τις αμέσως. Αν δε γνωρίζετε πώς να το κάνετε μόνοι σας, ζητήστε βοήθεια από τους φίλους σας ή από κάποιον ειδικό. Κάποιες ενημερώσεις καλύπτουν τις αδυναμίες του λογισμικού που εκμεταλλεύονται οι εγκληματίες. Σε κάποιες περιπτώσεις, το να μην εγκατασταθεί η ενημέρωση αρκεί για να αποκτήσει κάποιος πρόσβαση στον υπολογιστή σας.
- Φροντίστε για την ασφάλεια σας. Αξιολογήστε το λογισμικό που χρησιμοποιείτε και κάνετε τακτικά έλεγχο του υπολογιστή σας για την ύπαρξη κακόβουλων προγραμμάτων. Τα πιο σύνθετα και εξελιγμένα κακόβουλα προγράμματα μπορούν να διεισδύσουν στον υπολογιστή σας πριν καν

προστεθούν σε βάσεις δεδομένων antivirus.

- Δώστε προσοχή στις αναφορές σχετικά με τις απειλές για τα δίκτυα και τους νέους τύπους διαδικτυακής απάτης. Το Διαδίκτυο είναι γεμάτο απειλές και απάτες: phishing, ιοί Trojan που χρησιμοποιούνται για εκβιασμό, ψεύτικο λογισμικό antivirus, SMS phishing, ψεύτικα e-mail από τους φίλους σας σε ιστοσελίδες κοινωνικής δικτύωσης, καθώς επίσης και “κλασικά” e-mail που σας ενημερώνουν ότι κερδίσατε ένα διαγωνισμό, e-mail με ενδιαφέροντα “συνημμένα” αρχεία και συνδέσμους ICQ. Περιορίστε τον όγκο των προσωπικών πληροφοριών που είναι δημοσίως προσβάσιμες (συμπεριλαμβανομένων των πληροφοριών που αναρτώνται σε δημοφιλείς ιστοσελίδες κοινωνικής δικτύωσης, όπως το MySpace και το Facebook). Αυτού του είδους οι πληροφορίες μπορούν να χρησιμοποιηθούν από τους κυβερνοεγκληματίες εναντίον σας. ⓘ