Είμαστε όλοι ψηφιακά γυμνοί! (Καφαντάρης Τάσος)

Categories : ΚΟΙΝΩΝΙΑ

Date : 3 Μαρτίου, 2015

Η Πληροφορική υποτίθεται ότι βρίσκεται στα πρόθυρα συγκλονιστικής μετεξέλιξης: κβαντικοί υπολογιστές επί θύραις, «νέφη λογισμικού» συνδεδεμένα με υπερυπολογιστές που υπόσχονται παγκόσμια τεχνητή υπερνοημοσύνη και «Διαδίκτυο των Πάντων» όπου θα μας δίνει δεδομένα ακόμη και... το παπούτσι μας. Ομως, κάτι πάει θεόστραβα σε αυτό το Βασίλειο των Δεδομένων. Οι απανωτές αποκαλύψεις που ξεκίνησαν με την εξέγερση συνείδησης του πρώην πράκτορα της NSA Εντουαρντ Σνόουντεν έφθασαν τώρα σε ένα λεπτομερειακό ξεμπρόστιασμα του πώς η Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ είναι σε θέση να μπολιάζει στον υπολογιστή του καθενός μας προγράμματα κατασκοπείας αδιόρατα από οποιοδήποτε «ψηφιακό αντιβιοτικό». Η ανασφάλειά μας είναι τόσο τραγική ώστε οι ερευνητές που ανακάλυψαν τον μηχανισμό αυτόν να προειδοποιούν ότι «η μόνη λύση είναι να πετάξετε τον σκληρό σας δίσκο». Και σαν να μην έφτανε αυτό, μας αποκάλυψαν – συνεργαζόμενοι με την Interpol – ότι και οι μη κρατικοί απατεώνες είναι σε θέση να κλέβουν δισεκατομμύρια από τις τράπεζες όλου του πλανήτη, παραμένοντας ασύλληπτοι. Διαβάστε στις σελίδες μας το «πόσο γυμνοί είμαστε» και αποφασίστε για το «πόσο εξαρτημένοι πρέπει να είμαστε» από την Πληροφορική.

Από τη Δευτέρα, 16 Φεβρουαρίου 2015, δεν υπάρχει πλέον ούτε το έσχατο φύλλο συκής, η εσχάτη ψευδαίσθηση ότι ο υπολογιστής μας και τα προσωπικά μας δεδομένα που φυλάσσονται σε αυτόν βρίσκονται υπό τον έλεγχό μας. Ηταν αρκετή μία παρουσίαση σε διεθνές συνέδριο στο Μεξικό και η ανάρτηση στο Διαδίκτυο 40 σχετικών σελίδων από τη ρωσική εταιρεία ασφαλείας υπολογιστών Kaspersky για να αποκαλυφθεί ο μηχανισμός διακόρευσης κάθε ψήγματος πνευματικής ιδιοκτησίας που μας απέμενε. Ποιος ήταν ο δράστης τού κατά συρροήν και κατ' εξακολούθησιν εγκλήματος; Η αναφορά της Kaspersky δεν τον ονομάτιζε, αλλά έδινε «τις συντεταγμένες του». Ακολουθώντας τις, το πρακτορείο *Reuters* έφτασε σε μαρτυρίες και βροντοφώναξε την επόμενη ημέρα: η Υπηρεσία Εθνικής Ασφαλείας των ΗΠΑ (NSA) είναι ο Μεγάλος Αδελφός.

Ταυτόχρονα, στις 16 Φεβρουαρίου, μάθαμε για τον αντισυστημικό «Μικρό Αδελφό»: μια χακεροσυμμορία ονόματι Carnabak ξάφρισε σε διάστημα δύο ετών 1 δισεκατομμύριο δολάρια(!) από 100 τράπεζες, χωρίς καμιά τους να τους πιάσει στα πράσα.

Με τα προσωπικά μας δεδομένα σε «γυμνούς» υπολογιστές και τα χρήματά μας σε «ορθάνοιχτες» τράπεζες, σε τι αιώνα οδεύουμε;

Κατασκοπεία στην «καρδιά του κρεμμυδιού»

Δεν περνάει μήνας - ή, μάλλον, εβδομάδα... ίσως και μέρα - χωρίς να ανακύψει κάποια τρανταχτή είδηση για παραβίαση ψηφιακών απορρήτων. Αυτό όμως που εκτυλίσσεται από την περασμένη Δευτέρα είναι μια ειδησεογραφία αντάξια του καλύτερου σεναρίου κατασκοπείας. Το κακό είναι ότι δεν είναι μυθιστορία και δεν αφορά μόνον «κακούς», αλλά ίσως και τον οποιονδήποτε από μας.

Ένας παγκόσμιος πόλεμος υποκλοπής δεδομένων μαίνεται στον πλανήτη μας

Ας ξεκινήσουμε με το ποιος αποκάλυψε τη φοβερή ιστορία. Είναι μια πασίγνωστη διεθνώς εταιρεία προγραμμάτων ασφάλειας υπολογιστών, η Kaspersky Lab. Προβαίνει τακτικά σε διαλευκάνσεις υποθέσεων παραβιαστών (χάκερ) και θεωρείται εξαιρετικά αξιόπιστη, ιδιαίτερα λόγω του ότι... δεν έχει συμπάθειες στις κρατικές υπηρεσίες των ΗΠΑ. Γιατί αυτό το τελευταίο; Επειδή ο ιδρυτής και διευθύνων σύμβουλός της, ονόματι Ευγένιος Κασπέρσκι, είχε σπουδάσει κρυπτογραφία σε σχολείο της KGB και είχε εργασθεί στην ανάλογη υπηρεσία του ρωσικού στρατού. Ωστόσο, όποτε η Kaspersky προβαίνει σε αποκαλύψεις, φροντίζει να τις τεκμηριώνει με αδιάσειστα στοιχεία, οπότε...

Στην παρουσίαση της Δευτέρας η Kaspersky ολοκλήρωσε κατ' ουσίαν τη διαλεύκανση μιας υπόθεσης που είχε ξεκινήσει να ψάχνει από το 2012 (βλ. www.tovima.gr/science/article/?aid=462507).
Τότε είχε εντοπίσει ότι οι ιοί Flame και Stuxnet - που είχαν «χτυπήσει» τις ιρανικές πυρηνικές εγκαταστάσεις μέσω των συστημάτων αυτοματισμού της Siemens - είχαν φτιαχτεί από τη συνέργεια των ειδικών της αμερικανικής NSA και του ισραηλινού Σώματος Κυβερνοπολέμου. Αλλά το πώς ακριβώς είχαν εξελιχθεί αυτοί οι ιοί, με τι προγραμματιστικά εργαλεία και με ποιο «βελησεκές», ήταν κάτι που μπόρεσε να ξεδιαλύνει μόλις πρόσφατα.

Για να καταλάβουμε τα όσα αποκάλυψε, ας θυμηθούμε το τι κάνει ο υπολογιστής μας όταν ξεκινά: πρώτα διαβάζει τον «Δεκάλογο των εντολών» που λέγεται BIOS, αμέσως μετά ελέγχει τα υποσυστήματά του διαβάζοντας τα ενδόμυχα προγράμματα λειτουργίας της κάθε συσκευής (το λεγόμενο firmware) και έπειτα μπαίνει στο γνωστό μας λειτουργικό σύστημα και τις εφαρμογές που έχουμε εγκαταστήσει στον σκληρό μας δίσκο. Τα όποια «ψηφιακά αντιβιοτικά» χρησιμοποιούμε για την καταπολέμηση ιών περνούν από ψιλό κόσκινο τα πάντα εκτός από το firmware των συσκευών, που είναι μυστικό του κατασκευαστή της εκάστοτε συσκευής. Ιδιαίτερα αυτή η μυστικότητα του firmware είναι επτασφράγιστη στην περίπτωση των σκληρών δίσκων που φιλοξενούν τα δεδομένα μας.

Πώς «αλώθηκε» ο σκληρός

Τι κάνει λοιπόν ο καλός κατάσκοπος που θέλει να διεισδύσει στον υπολογιστή του «εχθρού», αλλά εκείνος τον έχει «στεγανοποιήσει» αποκόβοντας κάθε επικοινωνία του με το Διαδίκτυο; Οπως ανακάλυψε περιδεής η Kaspersky - και το επιβεβαίωσε το *Reuters* με μαρτυρία πρώην στελεχών της NSA - η Υπηρεσία Εθνικής Ασφαλείας των ΗΠΑ φροντίζει να αποκτά τον μυστικό κωδικό του firmware, ώστε οι ιοί που εμφυτεύει να φωλιάζουν στον σκληρό δίσκο και να μην ξεριζώνονται ποτέ. Πώς αποκτά αυτούς τους κωδικούς; Πολύ απλά - όπως εξήγησαν στο *Reuters* - στήνουν μια παραγγελία των συγκεκριμένων δίσκων από το Πεντάγωνο και στέλνουν κάποιους «ειδικούς» να τσεκάρουν το ότι οι συγκεκριμένοι δίσκοι είναι ασφαλείς, ζητώντας το πηγαίο πρόγραμμα του firmware. Δημιουργούν ένα αντίγραφο, στο οποίο μπολιάζουν τον επιθυμητό ιό, και φροντίζουν όποτε ο «εχθρός» παραγγείλει κάποιον σκληρό δίσκο να αλλάξουν το firmware προτού τον παραλάβει. Από εκεί και μετά ο υπολογιστής του τούς ανήκει. Ο ιός του firmware είναι ικανός να μολύνει τον υπολογιστή ξανά και ξανά, ακόμη κι αν σβήσει κανείς «οριστικά» τα περιεχόμενα του σκληρού δίσκου. «Είναι ικανός να ανασταίνεται συνεχώς» δήλωσε χαρακτηριστικά ο ρουμάνος επικεφαλής ερευνητής της Kaspersky, Κοστίν Ράιου (Costin Raiu). Και συμπλήρωσε: «Για τους περισσότερους σκληρούς δίσκους υπάρχουν λειτουργίες εγγραφής στο firmware, αλλά δεν υπάρχουν λειτουργίες ανάγνωσής του. Αυτό σημαίνει ότι είμαστε πρακτικά τυφλοί και δεν μπορούμε να ανιχνεύσουμε σκληρούς δίσκους που έχουν μολυνθεί από τέτοιον ιό».

Η εξίσωση Equation

Χακάροντας τις οθόνες

υπαλλήλων τραπεζών, οι ψηφιακοί ληστές ξάφρισαν 1 δισ. δολάρια από 100 τράπεζες μέσα σε δύο χρόνια - και παραμένουν άφαντοι!

Στη διαλεύκανση του προγραμματιστικού μηχανισμού της ψηφιακής κατασκοπείας η Kaspersky έφτασε με αφορμή ακριβώς την αντιπάθεια προς αυτήν των υπηρεσιών των ΗΠΑ: Ο κάτοχος ενός μολυσμένου υπολογιστή από ερευνητικό ίδρυμα χώρας της Μέσης Ανατολής κατέφυγε σε αυτούς για να βρει τι του είχαν φυτέψει. Ψάχνοντας τον σκληρό του δίσκο, οι ερευνητές της Kaspersky είδαν ότι τίποτε δεν θύμιζε τους ιούς των περίπου 60 ομάδων χάκερ που παρακολουθούν διεθνώς, εκτός από τα ίχνη που είχε αφήσει ο ιός Stuxnet. Αρχισαν να συλλέγουν μεθοδικά κάθε παρόμοιο στοιχείο, να καταγράφουν τη «χρονοσφραγίδα του» και να το συσχετίζουν με οτιδήποτε στο Διαδίκτυο. Κατέληξαν στο ότι η συγκεκριμένη οικογένεια ιών - που την βάφτισαν «Equation group» - είχε πιθανότατα ξεκινήσει να στήνεται το 1996 και πρωτοεκδηλώθηκε το 2001, αλλά σίγουρα άρχισε να δρα επιθετικότερα από το 2008 (τη χρονιά που ο Ομπάμα έγινε πρόεδρος των ΗΠΑ). Οι χώρες που έγιναν στόχοι των προγραμμάτων της ήταν περισσότερες από 30, μεταξύ των οποίων το Ιράν, η Ρωσία, η Συρία, το Αφγανιστάν, το Καζακστάν, το Πακιστάν, η Κίνα, το Μάλι, η Υεμένη, η Αλγερία, η Γαλλία, η Γερμανία, η Βραζιλία, η Ινδία και οι ίδιες οι ΗΠΑ, σε υπολογιστές που ανήκαν κυρίως σε κυβερνητικές και στρατιωτικές υπηρεσίες, πρεσβείες, τηλεπικοινωνιακούς φορείς, ερευνητικά ιδρύματα και ισλαμικά ιεροδιδασκαλεία. Κατά τους υπολογισμούς τους ο ρυθμός των «χτυπημάτων» ήταν (και είναι) περίπου 2.000 υπολογιστές τον μήνα.

Ο τρόπος διείσδυσης των ιών της οικογένειας Equation δεν περιορίζεται μόνο στην υποκατάσταση του firmware των σκληρών δίσκων: μόλυναν CD και μνήμες USB, εμφυτεύονταν ως εικόνες σε διαδικτυακούς κόμβους και διαχέονταν διαδικτυακά μέσω ενός προγράμματος-ιού ονόματι Fanny. Αυτό το τελευταίο εκμεταλλευόταν τα ίδια προγραμματιστικά λάθη που εκμεταλλευόταν ο Stuxnet, πράγμα που επιβεβαίωσε τις υποψίες των ερευνητών. «Είναι πολύ πιθανό», δήλωσε ο Ράιου, «να ήταν το Funny ο ανιχνευτής που εντόπισε τους υποψήφιους στόχους στο Ιράν για λογαριασμό του Stuxnet. Οι κατασκευαστές αυτών των προγραμματιστικών ιών σίγουρα σχετίζονται, αν δεν είναι η ίδια ακριβώς ομάδα». «Πάντως», συμπλήρωσε, «είναι σίγουρα ό,τι πιο εξελιγμένο έχουμε δει ως σήμερα, με κρυπτογραφικές μεθόδους παρασάγγες μπροστά από όλους τους άλλους χάκερ». Η Kaspersky απέφυγε σκόπιμα να ξεστομίσει η ίδια το όνομα της NSA, έστω κι αν το έπραξε έμμεσα με τη συσχέτιση Equation-Stuxnet. Το έκανε το *Reuters*, με τις μαρτυρίες δύο πρώην πρακτόρων. Αλλά για όποιον έχει παρακολουθήσει την υπόθεση Snowden, τον δράστη τον έχει ήδη ονοματίσει από τον Δεκέμβριο 2013 το γερμανικό περιοδικό *Der Spiegel*, βάσει απόρρητων εγγράφων που του είχε διοχετεύσει ο πρώην πράκτορας της NSA, Edward Snowden: είναι το Γραφείο Επιχειρήσεων Ειδικής Πρόσβασης της

NSA, TAO (Tailored Access Operations).

Ο τύπος των ήλων

Η κατηγορία είναι λοιπόν στοιχειοθετημένη και ο ένοχος καταδείχθηκε έμμεσα, άμεσα και επώνυμα. Τι είχε να πει ο ίδιος ο κατηγορούμενος; «Είμαστε ενήμεροι για την πρόσφατα δημοσιευθείσα έκθεση. Δεν πρόκειται να σχολιάσουμε δημόσια τυχόν ισχυρισμούς που η έκθεση εγείρει, ή να συζητήσουμε οποιεσδήποτε λεπτομέρειες» ήταν η απάντηση εκπροσώπου της NSA στο αμερικανικό περιοδικό *The Inquirer*.

Οπως κι αν ερμηνεύσετε αυτή τη δήλωση, το θέμα είναι πως οι μετασεισμικές δονήσεις των αποκαλύψεων γίνονται ήδη αισθητές. «Αν αυτοί οι ισχυρισμοί είναι αληθινοί», δήλωσε στο ίδιο περιοδικό ο Τζον Τσέιμπερς, αφεντικό της κατασκευάστριας τηλεπικοινωνιακών συστημάτων Cisco, «τέτοιου είδους ενέργειες θα υπονομεύσουν την εμπιστοσύνη στον κλάδο μας και την ικανότητά του να παρέχει προϊόντα διεθνώς. Πολύ απλά, δεν μπορούμε να δουλέψουμε με τέτοιο κλίμα. Οι πελάτες μας μάς εμπιστεύονται για το ότι θα τους παραδώσουμε προϊόντα που πληρούν τα υψηλότερα πρότυπα ακεραιότητας και ασφάλειας». Στο ίδιο μήκος κύματος, ο σύμβουλος του προέδρου των ΗΠΑ σε θέματα τεχνολογίας Πληροφοριών και Επικοινωνιών, Peter Swire, δήλωσε στο *Reuters* πως «η έκθεση της Kaspersky έδειξε ότι είναι σημαντικό για τη χώρα μας να εξετάζει τις πιθανές επιπτώσεις στο εμπόριο και τις διπλωματικές σχέσεις πριν αποφασίσει να αξιοποιήσει για τη συγκέντρωση πληροφοριών τις γνώσεις της σχετικά με ρωγμές του λογισμικού».

Οι αντιδράσεις αυτές έχουν να κάνουν με την ανατριχίλα του επιχειρηματικού κόσμου των ΗΠΑ ότι θα αποκλειστούν από πολλές αγορές. Ηδη η Κίνα ζητεί για τα πληροφορικά συστήματα των τραπεζών της οι υποψήφιοι προμηθευτές να της υποβάλουν τον πηγαίο κώδικα του firmware που τα συνοδεύει. Τι θα συμβεί αν η δυσπιστία επεκταθεί και αρχίσουν όλοι να ζητούν τόσο «βαθιές» τεχνολογικές διασφαλίσεις;

Το μεγαλύτερο ψηφιακό ριφιφί

Το σοκ των αποκαλύψεων της Kaspersky περί κρατικής ψηφιακής κατασκοπείας διπλασιάστηκε την ίδια αποφράδα ημέρα με την αποκάλυψη - επίσης από την ίδια εταιρεία - για τον βαθμό ψηφιακής κατασκοπείας στον οποίο έχουν φθάσει και οι ιδιώτες απατεώνες: Μια ομάδα ατόμων από τη Ρωσία, την Ουκρανία, την Κίνα και διάφορες χώρες της Ευρώπης είχε αναπτύξει ιούς παρακολούθησης των ενεργειών τραπεζικών υπαλλήλων, ώστε αργότερα να προβαίνουν σε τραπεζικές συναλλαγές «σαν κύριοι». Το αποτέλεσμα ήταν να «αρμέξουν» μέσα σε δυο χρόνια ένα δισεκατομμύριο δολάρια από 100 τράπεζες και χρηματοοικονομικούς οργανισμούς στη Ρωσία, τις ΗΠΑ, τη Γερμανία, την Κίνα, την Ουκρανία, τον Καναδά, το Χονγκ Κονγκ, την Ταϊβάν, τη Ρουμανία, τη Γαλλία, τη Νορβηγία, την Ινδία, το Ηνωμένο Βασίλειο, την Πολωνία, το Πακιστάν, το Νεπάλ, το Μαρόκο, την Ισλανδία, την Ιρλανδία, την Τσεχία, την Ελβετία, τη Βραζιλία, τη Βουλγαρία και την Αυστραλία.

Το όλο κόλπο ξεκίνησε το 2013, με την εμφύτευση του ιού ονόματι Carbanak σε υπολογιστές εργαζομένων σε τράπεζα. Από εκεί οι απατεώνες ήταν σε θέση να διεισδύσουν στο εταιρικό δίκτυο της τράπεζας, να εντοπίσουν τους υπολογιστές των διαχειριστών του και να προχωρήσουν σε παρακολούθηση μέσω video. Αυτό τους επέτρεπε να βλέπουν και να καταγράφουν ό,τι συνέβαινε στις οθόνες του προσωπικού που ασχολούνταν με τα συστήματα μεταφοράς χρημάτων. Με αυτό τον τρόπο, οι απατεώνες μπορούσαν να μάθουν μέχρι και την τελευταία λεπτομέρεια για τις τραπεζικές διαδικασίες και να μιμηθούν τις δραστηριότητες του προσωπικού ώστε να μεταφέρουν και να ρευστοποιήσουν χρηματικά ποσά. Για παράδειγμα, αν ένας λογαριασμός είχε 1.000 δολάρια, οι απατεώνες άλλαζαν την αξία του σε 10.000 δολάρια και έπειτα μετέφεραν τα 9.000 σε δικούς τους λογαριασμούς. Ο κάτοχος του λογαριασμού δεν υποπτευόταν ότι υπήρχε κάποιο πρόβλημα, γιατί το κεφάλαιο των 1.000 δολαρίων ήταν ακόμη εκεί. Επιπλέον, οι εγκληματίες αποκτούσαν τον έλεγχο των ATM των τραπεζών και μέσω εντολών τα ρύθμιζαν ώστε να πληρώνουν μετρητά σε προκαθορισμένα χρονικά διαστήματα. Οταν ερχόταν η στιγμή της «εθελοντικής πληρωμής», ένα από τα παλικάρια της συμμορίας φρόντιζε να είναι δίπλα στο μηχάνημα για να εισπράξει.

Η πρώτη «ληστεία της οθόνης»

«Οι ληστείες αυτές αποτέλεσαν έκπληξη» δήλωσε ο αρμόδιος ερευνητής της Kaspersky, Σεργκέι Γκολοβάνοφ, «γιατί για τους απατεώνες δεν έπαιζε κανένα ρόλο τι λογισμικό χρησιμοποιούσαν οι τράπεζες. Οπότε, ακόμη κι αν μια τράπεζα χρησιμοποιεί ένα ειδικά γραμμένο γι' αυτήν λογισμικό, δεν είναι ασφαλής: Οι εγκληματίες δεν χρειάστηκε καν να χακάρουν τις ηλεκτρονικές υπηρεσίες των τραπεζών. Μόλις αποκτούσαν πρόσβαση στο δίκτυο, μάθαιναν πώς να κρύψουν τις κακόβουλες δράσεις τους πίσω από νόμιμες ενέργειες».

Το ακόμη πιο εκπληκτικό όμως μάλλον είναι το ότι η Kaspersky διαλεύκανε μεν το μυστήριο για λογαριασμό της Interpol, αλλά οι «Ρομπέν των τραπεζών» παραμένουν άγνωστοι ως πρόσωπα, ασύλληπτοι και συνεχίζουν τη δράση τους!

Ο απόηχος αυτών των δύο «αποκριάτικων αποκαλύψεων» δεν μπορεί παρά να είναι σκέψεις - μαύρες σκέψεις. Διότι, πώς να εφησυχάσεις ότι η όποια NSA σε παρακολουθεί «για το καλό σου»; Πώς να δεχτείς ότι τα πάντα όσα γράφεις και καταχωρείς στον υπολογιστή σου - ιδέες, σχόλια, προσωπικές απόψεις και εμπειρίες, πνευματικά έργα - είναι ανά πάσα στιγμή προσβάσιμα από αθέατους κατασκόπους, που ποιος ξέρει για ποιον πραγματικά δουλεύουν; Κι έπειτα, αν τα τσακάλια όπου Γης μπορούν και ξαφρίζουν δισεκατομμύρια από τους φύλακες των οικονομιών μας, τις τράπεζες, ποια διασφάλιση έχει ο μισθός σου, η αποταμίευσή σου, η ίδια η οικονομία ατόμων και κρατών; Και όταν, πολύ σύντομα, ο πλανήτης γεμίσει αισθητήρες και το Διαδίκτυο των Υπολογιστών μεταβληθεί σε Διαδίκτυο των Πάντων, τι θα απομείνει πραγματικά δικό σου, στον έλεγχό σου, μυστικό σου;

Το φάσμα της «τεχνοφοβίας»

Η αγωνία αυτή δεν είναι μόνο η αγωνία ενός απλού πολίτη. Την ίδια αγωνία εξέφρασαν ακόμη και αυτοί οι ερευνητές της Kaspersky, όταν δημοσίευσαν - στις 22 Ιανουαρίου 2015 - τις προβλέψεις τους για τον κόσμο μας εν έτει 2045. Πλάι στη σιγουριά τους για το ότι «τα ρομπότ θα βρίσκονται παντού γύρω μας», «τα σώματά μας θα είναι γεμάτα αισθητήρες

και νανορομπότ», «τα σπίτια μας θα είναι υπερέξυπνα», «οι τρισδιάστατοι εκτυπωτές θα παράγουν τα πάντα, πάμφθηνα» και ότι «όλοι οι υπολογισμοί θα γίνονται από το Ψηφιακό Νέφος» ή ότι «μια τεχνητή υπερνοημοσύνη θα μας φροντίζει μέσω Διαδικτύου», προσέθεσαν και τη γιγαντωμένη τεχνοφοβία. «Δεν θα είναι όλοι ενθουσιασμένοι από τον νέο, γενναίο ρομποτικό κόσμο» έγραψαν. «Νέοι Λουδίτες πιθανόν θα προκύψουν για να αντιταχθούν στην ανάπτυξη των έξυπνων σπιτιών, τον αυτοματοποιημένο τρόπο ζωής και τα ρομπότ. Η αντίθεση στις εξελίξεις της πληροφορικής θα τους κάνει να απορρίψουν τη χρήση έξυπνων συστημάτων, συσκευών και ρομπότ και θα αρνηθούν να έχουν την οποιαδήποτε ψηφιακή ταυτότητα».

Χμμμ... εδώ που τα λέμε, όλο και πιο πολύ αρχίζουμε να πιστεύουμε τελευταία ότι ο καταναλωτικός πολιτισμός μας κάνει, θαρρείς, τα πάντα για την επιστροφή σε έναν θρησκόληπτο μεσαίωνα. Μάλλον δεν είναι η «τεχνητή υπερνοημοσύνη» που μας λείπει, αλλά η ανθρώπινη σύνεση και σοφία.

Μόνο τα Windows γίνονται στόχοι;

Κατά τα λεγόμενα της Kaspersky: «Ολο το κακόβουλο λογισμικό που έχουμε συλλέξει μέχρι στιγμής έχει σχεδιαστεί για να λειτουργεί με το λειτουργικό σύστημα Windows της Microsoft. Ωστόσο, υπάρχουν ενδείξεις ότι υπάρχουν εκδόσεις του και για συστήματα μη Windows. Για παράδειγμα, ένας από τους διαδικτυακούς κόμβους επικοινωνίας της ομάδας Equation λαμβάνει επί του παρόντος δεδομένα από μια μεγάλη δεξαμενή θυμάτων του στην Κίνα, που φαίνεται ότι είναι υπολογιστές Apple με λειτουργικό σύστημα Mac OS X. Αυτό μας οδηγεί στο συμπέρασμα ότι υπάρχει έκδοση για Mac. Επιπρόσθετα, παρατηρήσαμε ότι ένα από τα κακόβουλα λογισμικά, σε μορφή PHP script, παίρνει ιδιαίτερες προφυλάξεις ώστε να "μεταμφιέζεται" σε τύπο αρχείου HTML για iPhone. Το ότι ανακατευθύνει τους χρήστες iPhone στον συνεργαζόμενο με την Equation διακομιστή υποδηλώνει την ικανότητα μόλυνσης και των iPhone».

Πώς δουλεύει η Equation

Στους ήδη γνωστούς κατασκοπευτικούς κυβερνοϊούς Stuxnet, Flame και Gauss

η έρευνα της Kaspersky προσέθεσε έξι ακόμη μέλη της οικογένειας Equation: τον Funny, τον DoubleFantacy, τον TripleFantacy και τους EquationLaser, EquationDrug και GrayFish. Ο καθένας τους επιτελεί ξεχωριστό ρόλο, αλλά εκείνος που εξέπληξε με την πολυπλοκότητά του τους ερευνητές ήταν ο GreyFish, που χειρίζεται την όλη «κοπτορραπτική» των σκληρών δίσκων. Οπως διαβάζουμε στην αναφορά τους (http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf):
«Οταν ξεκινά ο υπολογιστής, ο GrayFish επιτελεί πειρατεία στους μηχανισμούς φόρτωσης του λειτουργικού συστήματος, φυτεύοντας τον κώδικά του στο αρχείο εκκίνησης (boot record). Αυτό του επιτρέπει να ελέγχει κάθε στάδιο της εκκίνησης των Windows. Στην πράξη, μετά τη μόλυνση, ο υπολογιστής δεν τρέχει πια μόνος του: είναι ο GrayFish που τον τρέχει βήμα προς βήμα, κάνοντας τις απαραίτητες αλλαγές στο φτερό. Μετά την εκκίνηση των Windows, ο GrayFish ξεκινά έναν μηχανισμό αποκρυπτογράφησης τεσσάρων ως πέντε σταδίων, προκειμένου να διασφαλίσει την εκτέλεση κώδικα στο περιβάλλον των Windows. Κάθε στάδιο αποκωδικοποιεί και εκτελεί το επόμενο και ολόκληρη η πλατφόρμα θα ξεκινήσει μόνο μετά την επιτυχή εκτέλεση όλων των σταδίων. Για να αποθηκεύσει τις κλεμμένες πληροφορίες - όπως και τις δικές του βοηθητικές πληροφορίες - ο GrayFish εφαρμόζει το δικό κρυπτογραφημένο εικονικό σύστημα αρχείων (VFS) στο εσωτερικό του μητρώου των Windows. Για να παρακάμψει τους μηχανισμούς ασφαλείας του λειτουργικού συστήματος, εκμεταλλεύεται πολλούς νόμιμους οδηγούς, όπως έναν από το πρόγραμμα CloneCD. Ο GrayFish αποθηκεύει τα κλεμμένα δεδομένα σε κρυπτογραφημένη μορφή στο μητρώο καταχώρισης (registry), τα αποκρυπτογραφεί δυναμικά και τα εκτελεί».

Οσο για τον κυβερνοϊό Funny, που δημιουργήθηκε το 2008 με στόχο τη μέση Ανατολή και χώρες της Ασίας, οι ερευνητές της Kaspersky γράφουν: «Ο κύριος σκοπός του Funny φαίνεται ότι ήταν η χαρτογράφηση των "στεγανών" δικτύων. Για τον σκοπό αυτόν χρησιμοποιεί μια μοναδική εντολή και μηχανισμό ελέγχου που βασίζονται στη λειτουργία των USB. Οταν μια μνήμη USB έχει μολυνθεί, ο Funny δημιουργεί έναν κρυφό αποθηκευτικό χώρο μέσα του. Επίσης, αν αποθηκευτούν εντολές "επίθεσης στον υπολογιστή" σε αυτόν τον χώρο, ο Funny τις αναγνωρίζει και τις εκτελεί. Αν ο ιός μολύνει υπολογιστή που δεν έχει σύνδεση στο Διαδίκτυο, συλλέγει τις βασικές πληροφορίες του συστήματος (τον χάρτη της υποδομής του) και τις αποθηκεύει στην κρυφή περιοχή. Αργότερα, όταν το USB μπει σε υπολογιστή συνδεδεμένο στο Διαδίκτυο, ο ιός φροντίζει να συλλεχθούν τα δεδομένα από την κρυφή περιοχή και να αποσταλούν σε ειδικούς διαδικτυακούς κόμβους που ελέγχονται από την Equation group».

Οσον αφορά τους τύπους και τις μάρκες σκληρών δίσκων που έχει διαβρώσει μέχρι στιγμής η Equation είναι μια λίστα που πρακτικά τους περιλαμβάνει όλους: WDC WD, ST, Maxtor STM, SEAGATE ST, SAMSUNG, IC, IBM, Hitachi, HTS, HTE, HDS, HDT, ExcelStor, C300, M4, OCZ, OWC, Corsair, Mushkin, TOSHIBA M. Η διείσδυση γίνεται μέσω εντολών ATA του firmware.

(Πηγή: tovima.gr/science/)