Η NSA είχε 12 άτομα να παρακολουθούν το VPN της ελληνικής κυβέρνησης

φωτό: δωμάτιο παρακολουθήσεων της Στάζι – αναπαράσταση στο DDR Museum

Τη μέρα που η ελληνική ειδησεογραφία περιστρέφεται –δικαίως- γύρω από το αποτέλεσμα της τρίτης και τελευταίας ψηφοφορίας για εκλογή νέου Προέδρου της Δημοκρατίας (το οποίο συνεπάγεται άμεσες εκλογές) υπάρχει μια είδηση που μέχρι στιγμής δεν έχει καταφέρει να περάσει ούτε καν στα ψιλά των εγχώριων ΜΜΕ: Σύμφωνα με το νέο πακέτο διαρροών από τη δράση της NSA, που έρχεται σταδιακά στο φως χάρη στον Έντουαρντ Σνόουντεν, η

Εθνική Υπηρεσία Ασφαλείας των ΗΠΑ έσπαγε τα συστήματα κρυπτογράφησης των δικτύων **VPN ("virtual private networks", δηλαδή εικονικών ιδιωτικών δικτύων)**, τα οποία θεωρούνται η ασφαλέστερη οδός επικοινωνίας για οργανισμούς όπως οι κυβερνήσεις κρατών, προκειμένου να τις παρακολουθεί. **Η λεπτομέρεια που θα πληροφορηθεί κάπως αργά η απερχόμενη ελληνική κυβέρνηση, είναι ότι μόνο για το VPN που υποτίθεται ότι θα διασφάλιζε τη μυστικότητα των επικοινωνιών μεταξύ των μελών της, η NSA απασχολούσε 12 πράκτορές της.**

> *"One example is virtual private networks (VPN), which are often used by companies and institutions operating from multiple offices and locations. A VPN theoretically creates a secure tunnel between two points on the Internet. All data is channeled through that tunnel, protected by cryptography. When it comes to the level of privacy offered here, virtual is the right word, too. This is because the NSA operates a large-scale VPN exploitation project to crack large numbers of connections, allowing it to intercept the data exchanged inside the VPN – including,* ***for example, the Greek government's use of VPNs. The team responsible for the exploitation of those Greek VPN communications consisted of 12 people, according to an NSA document SPIEGEL has seen.***"
>
> *Απόσπασμα από την ανάρτηση του Der Spiegel (η υπογράμμιση από το Thecricket)*

Την αποκάλυψη φέρνει στο φως το περιοδικό Der Spiegel, στο τρέχον τεύχος του. Οι νέες διαρροές Σνόουντεν αφορούν τις μεθόδους που χρησιμοποιούν οι αμερικανικές και βρετανικές μυστικές υπηρεσίες καθώς και οι σύμμαχοί τους στο **"Five Eyes"** προκειμένου να σπάσουν και τα τελευταία επίπεδα ασφάλειας του Ίντερνετ και να έχουν πρόσβαση στα πάντα. Όπως αποδεικνύουν τα απόρρητα έγγραφα, **η NSA θεωρεί τα συστήματα κρυπτογράφησης**

«απειλή» για το έργο της, δηλαδή για την υποκλοπή πληροφοριών και την αντιμετώπιση κακόβουλων λογισμικών. Γι'αυτό επενδύει ιδιαίτερα στο σπάσιμό τους. Σε μεγάλο βαθμό τα έχει καταφέρει, ωστόσο **το αισιόδοξο είναι ότι υπάρχουν ακόμα συστήματα κρυπτογράφησης που την δυσκολεύουν**. Βέβαια, όπως επισημαίνουν, οι συντάκτες του Spiegel, τα συγκεκριμένα έγγραφα χρονολογούνται δύο χρόνια πίσω, οπότε μπορεί στο μεταξύ οι αμερικανοί και βρετανοί πράκτορες να έχουν σπάσει και τα τελευταία συστήματα.

Τα VPNs που πριν από είκοσι χρόνια χρησιμοποιούνταν κατά κύριο λόγο από κυβερνήσεις και μυστικές υπηρεσίες για τη διακίνηση απόρρητων πληροφοριών, είναι σήμερα διαθέσιμα σε όλους τους χρήστες που θέλουν ένα αυξημένο επίπεδο ασφαλείας στις επικοινωνίες τους από οποιοδήποτε μέρος του κόσμου. Τα χρησιμοποιούν τράπεζες, εταιρείες, πανεπιστήμια, ακόμη και ιδιώτες που δεν θέλουν να αφήσουν τις συναλλαγές τους εκτεθειμένες σε ενδεχόμενες παρακολουθήσεις. Επιπλέον, η ύπαρξή τους και το γεγονός ότι δεν είχε βρεθεί ακόμα ο τρόπος παραβίασής τους, δημιουργούσε σημαντικές δικλείδες ασφαλείας και ενάντια στο κοινό έγκλημα ή και σε πιο σοβαρές απειλές και επιθέσεις μέσω διαδικτύου.

Τις τελευταίες ώρες η διεθνής κοινότητα ειδικών σε ζητήματα διαδικτυακής ασφάλειας, τονίζει ότι για πρώτη φορά γίνεται γνωστό πώς ακριβώς η NSA έσπαγε τα συστήματα ασφαλείας των VPN και τα πρωτόκολλα **SSL** και **TLS**. Χαρακτηριστικό είναι το σχετικό τουίτ του Τζόναθαν Μάγιερ, στο μάθημα του οποίου βασίζεται η **σειρά των αναρτήσεων που κάνουμε στο thecricket για τη νομοθεσία των ΗΠΑ περί παρακολουθήσεων**:

> *Finally, some detail on how the NSA passively snoops SSL and VPNs. It targets protocols that lack forward secrecy. pic.twitter.com/BeM8xcJhFq*
>
> *— Jonathan Mayer (@jonathanmayer) December 28, 2014*

Επισημαίνουν επίσης τους κινδύνους που συνεπάγεται αυτή η δράση της NSA για την ασφάλεια όλων μας:

> *The spies have just about destroyed communications security. Criminals, in and out of govt, are thrilled. http://t.co/pEOvHQKTGQ — Dan Gillmor (@dangillmor) December 29, 2014*

Οι υποκλοπές μέσω παραβίασης των πρωτοκόλλων SSL και TLS, φαίνεται πως είναι κάτι παραπάνω από ρουτίνα για της μυστικές υπηρεσίες. **Για το 2012 στόχος της NSA ήταν να φτάσει τα 10 εκατομμύρια παραβιάσεις συνδέσεων μέσω https τη μέρα.** Έδειχναν μάλιστα ιδιαίτερο ενδιαφέρον για την στιγμή που οι χρήστες πληκτρολογούν τα password τους για να συνδεθούν σε δίκτυα και υπηρεσίες όπως τα Facebook, Twitter, Hotmail, Yahoo και το iCloud της Apple, ώστε να αποκωδικοποιήσουν τον τρόπο λειτουργίας των εφαρμογών κρυπτογράφησης, επισημαίνουν οι συντάκτες του Spiegel.

* * *

Όπως διαπιστώνεται, οι αμερικανοί πράκτορες διαχωρίζουν πέντε κλιμακούμενα επίπεδα δυσκολίας στο σπάσιμο των συστημάτων κρυπτογράφησης. Το “**trivial**” (μηδαμινό) αφορά κάτι όπως η καταγραφή της διαδρομής ενός εγγράφου που αποστέλλεται μέσω ίντερνετ. Η παρακολούθηση ενός τσατ στο Facebook θεωρείται “**minor** task”. Μέτριας δυσκολίας, δηλαδή “**moderate**”, είναι η αποκρυπτογράφηση email που στέλνονται μέσω του ρωσικού παρόχου ηλεκτρονικής αλληλογραφίας «mail.ru». Τα πράγματα δυσκολεύουν με την παρακολούθηση της ηλεκτρονικής αλληλογραφίας όσων χρησιμοποιούν παρόχους όπως το Zoho και το δίκτυο Tor (η πιο γνωστή και δωρεάν υπηρεσία που επιτρέπει στους χρήστες να πλοηγούνται στο διαδίκτυο διατηρώντας την ανωνυμία τους).

Τέτοιες παρακολουθήσεις θεωρούνται “**major**” (μεγάλης) δυσκολίας. Υπάρχουν, όμως και συστήματα τα οποία οι πράκτορες δεν μπορούν να τα σπάσουν και τα κατατάσσουν στο επίπεδο “**catastrophic**”. Τέτοια είναι, για παράδειγμα, ένας συνδυασμός ταυτόχρονης χρήσης του δικτύου Tor, με το σύστημα ανταλλαγής μηνυμάτων CSpace και το σύστημα ιντερνετικής τηλεφωνίας ZRTP (χρησιμοποιείται για την κρυπτογράφηση τηλεφωνημάτων και ανταλλαγής τσατ μέσω κινητών τηλεφώνων).

* * *

Υπενθυμίζουμε ότι η λειτουργία του προγράμματος παρακολουθήσεων της NSA βασίζεται στο Νόμο περί Παρακολουθήσεων Αντικατασκοπείας (Foreign Intelligence Surveillance Act ή FISA), ο οποίος νομιμοποίησε για πρώτη φορά τις μαζικές (bulk) υποκλοπές, εντός και εκτός συνόρων ΗΠΑ, για παρελθοντικές ή/και μελλοντικές επικοινωνίες. Στενοί συνεργάτες της NSA στο πρόγραμμα παρακολουθήσεων είναι οι μυστικές υπηρεσίες των άλλων χωρών μελών της συμφωνίας **“Five Eyes” (επισήμως “UKUSA Agreement”)**: η **GCHQ** της Μ.Βρετανίας, η **CSE** του Καναδά, η **ASD** της Αυστραλίας, και η **GCSB** της Ν.Ζηλανδίας.

Περισσότερα για το νομικό πλαίσιο, στην σχετική ανάρτηση **Παρακολουθήσεις εκτός συνόρων ή «για λόγους εθνικής ασφάλειας»**.