το θέμα της εβδομάδας

Υβριδικός πόλεμος και κυβερνοεπιθέσεις

Οι κυβερνοεπιθέσεις, που ήρθαν για να μείνουν, εντάσσονται στα πλαίσια μίας εκσυγχρονισμένης και εμπλουτισμένης μορφής συγκρούσεων, του υβριδικού πολέμου. Γενικό χαρακτηριστικό του υβριδικού πολέμου αποτελεί η ασυμμετρία των συρράξεων που διεξάγονται σε πολλά πεδία σε διάφορα χρονικά διαστήματα. Σ' αυτού του τύπου τις συγκρούσεις ο εκάστοτε παράγοντας, που μπορεί να μην είναι απλά ένα κράτος, μετέρχεται μεθόδους όπως οι κυβερνοεπιθέσεις, η προπαγάνδα μέσω των ΜΜΕ, η χρησιμοποίηση των μέσων κοινωνικής δικτύωσης ακόμα και για στρατολόγηση, οι τρομοκρατικές ενέργειες ή οι κοινές εγκληματικές ενέργειες.

Οι δυτικοί αναλυτές εντοπίζουν τέτοιες μεθόδους κύρια στις «αντι-δυτικές» δυνάμεις όπως ο ISIS. Ωστόσο, οι μέθοδοι που ακολουθούνται δεν αποτελούν «ευρεσιτεχνία» του Ισλαμικού Κράτους, καθώς χρησιμοποιήθηκαν πολλές απ' αυτές για χρόνια από το ΝΑΤΟ, την CIA και άλλες υπηρεσίας στους πολέμους που διεξήγαγαν αλλά και στις περιοχές που θέλησαν να ελέγξουν.

Ο όρος «υβριδικός πόλεμος» προσπαθεί να περιγράψει μία ολότητα στην οπτική των εμπλεκόμενων δυνάμεων, δηλαδή το ξεπέρασμα της συμβατικής σύγκρουσης στο πεδίο της μάχης και το χτύπημα κάθε τρωτού σημείου του αντιπάλου σε κάθε πιθανό επίπεδο.

Για να κατανοήσουμε κάποια από τα γνωρίσματά του αρκεί να σκεφτούμε κάποια από τα τελευταία επεισόδια στην πολεμική μεταξύ Ρωσίας και ΗΠΑ. Στις πρόσφατες αμερικανικές εκλογές όταν κατηγορήθηκαν οι Ρώσοι για προσπάθεια επηρεασμού του αποτελέσματος μέσω διαδικτυακών επιθέσεων, στήθηκε μία μηχανή προπαγάνδας από τα διάφορα πολιτικά στρατόπεδα στις ΗΠΑ που αφορούσε όχι μονάχα το εσωτερικό μέτωπο, αλλά και την ίδια την διεθνή κοινή γνώμη. Η πολεμική αυτή εκτυλίσσεται σε ένα βαθμό και στις εμπόλεμες ζώνες της Μέσης Ανατολής με τις δύο μεριές να μάχονται για την κυριαρχία στην περιοχή.

Γίνεται σαφές ότι στο διεθνές σκηνικό έχει στηθεί μία πολυπλόκαμη και πολυπαραγοντική διαμάχη που κάθε άλλο παρά δευτερεύοντα ρόλο παίζουν και οι μικρότερες δυνάμεις, όπως π.χ. η Τουρκία, το Ισραήλ και η Σαουδική Αραβία. Μάλιστα αρκετοί αναλυτές επισημαίνουν ότι η Τουρκία εδώ και καιρό διεξάγει υβριδικό πόλεμο εναντίον της Ελλάδας.

Ο όρος «υβριδικός πόλεμος» προσπαθεί να περιγράψει μία ολότητα στην οπτική των εμπλεκόμενων δυνάμεων, δηλαδή το ξεπέρασμα της συμβατικής σύγκρουσης στο πεδίο της μάχης και το χτύπημα κάθε τρωτού σημείου του αντιπάλου σε κάθε πιθανό επίπεδο

Κυβερνοπόλεμος: Ενός κακού, μύρια έπονται

Η πρόσφατη κυβερνοεπίθεση φέρνει στην επιφάνεια μία νέα διάσταση συγκρούσεων στο παγκόσμιο γίγνεσθαι

■ του **Βασίλη Γεροδήμου**

Η κυβερνοεπίθεση της περασμένης εβδομάδας έθεσε εκτός λειτουργίας τους μαγνητικούς τομογράφους στη Μ. Βρετανία, τα μηχανήματα αυτόματης πώλησης εισιτηρίων στους σιδηροδρόμους της Γερμανίας, υπολογιστές στο υπουργείο Εσωτερικών της Ρωσίας, καθώς και ένα μέρος του δικτύου της FedEx στις ΗΠΑ.

Τα θύματα του ιού «WannaCry» σε ολόκληρο τον κόσμο υπολογίζονται σε τουλάχιστον 200.000, με την πλειοψηφία των χρηστών που μολύνθηκαν να βρίσκεται σε Κίνα, Ρωσία, Ιαπωνία, Μ. Βρετανία και Βραζιλία. Το κενό ασφαλείας είχε εντοπιστεί από την αμερικανική Εθνική Υπηρεσία Ασφάλειας (NSA), η οποία ανέπτυξε προγράμματα διείσδυσης και παρακολούθησης βασισμένα στα κενά ασφαλείας των Windows. Κάποια από αυτά τα προγράμματα διείσδυσης της NSA κλάπηκαν πριν λίγο καιρό.

Ο ιός «WannaCry» επηρέασε μόνο υπολογιστικά συστήματα της Microsoft, η οποία έβγαλε μία ανανέωση ασφαλείας μετά την πρώτη εξάπλωση του ιού. Αυτή η ενημέρωση του λογισμικού για την εν λόγω ευπάθεια αφορούσε μόνο την τελευταία έκδοση του δημοφιλούς λογισμικού (Windows 10), πράγμα το οποίο εγείρει πολλά ερωτήματα για τον αμερικανικό κολοσσό, καθώς το 74% των χρηστών παγκοσμίως, συμπεριλαμβανομένων δημοσίων οργανισμών και εταιρειών, χρησιμοποιούν τις παλαιότερες εκδόσεις του λογισμικού.

Το ιστορικό και η εμπλοκή της NSA

Με τη βοήθεια ενός τρωτού σημείου στα Windows οι επιτιθέμενοι κατάφεραν να αποκτήσουν πρόσβαση στα μηχανήματα χιλιάδων χρηστών και με έναν αλγόριθμο κρυπτογράφησης, που προϋπήρχε, κατάφεραν να «κλειδώσουν» τα αρχεία τους. Για να τους δοθεί πρόσβαση στα αρχεία οι χρήστες έπρεπε να καταβάλουν ένα ποσό της τάξης των 300 δολαρίων σε ψηφιακό νόμισμα Bitcoin, για να μην μπορούν οι επιτιθέμενοι να εντοπιστούν από τις αρχές.

Πίσω από την μεγάλης κλίμακας διαδικτυακή επίθεση βρίσκεται μια ομάδα hackers με το όνομα «Shadow Brokers». Η ομάδα αυτή τον Απρίλιο διέρρευσε μια σειρά από διαδικτυακά «όπλα» που είχε στο «οπλοστάσιό» της η NSA, αποφασίζοντας να τα πουλήσει στο «Σκοτεινό Διαδίκτυο». Η κυβερνοεπίθεση αυτή θεωρείται ως μια προσπάθεια της ομάδας αυτής να διαφημίσει το υλικό που έχει στη διάθεση της για να μπορέσει να το πουλήσει στους υποψήφιους πελάτες της. Το υλικό αυτό, πέρα από εργαλεία διείσδυσης σε smartphones, λειτουργικά συστήματα κ.λπ., περιλαμβάνει και κλεμμένες πληροφορίες για τα πυρηνικά προγράμματα Κίνας, Ιράν, Ρωσίας και Βόρειας Κορέας.

Είναι λογικό ότι όπως και στον πραγματικό κόσμο, έτσι και στον κόσμο του διαδικτύου, ιδιαίτερα το τελευταίο διάστημα που έχει γίνει προέκταση της καθημερινότητάς μας, θα πραγματοποιούνται εγκληματικές ενέργειες. Είναι σαφές ότι η NSA είχε γνώση αυτού του κενού ασφαλείας, το εκμεταλλεύτηκε εντούτοις για να μπορεί να παρακολουθεί ανενόχλητη τους ανθρώπους που έχουν το συγκεκριμένο λειτουργικό σύστημα στους υπολογιστές τους. Ενώ ανεβαίνουν οι τόνοι εναντίον της υπηρεσίας και για το αν υπήρξε ή όχι κάποια μυστική συμφωνία με την Microsoft (που ουκ ολίγες φορές έχει συνεργαστεί με τις αμερικανικές αρχές) για να μην καλυφθεί το κενό ασφαλείας.

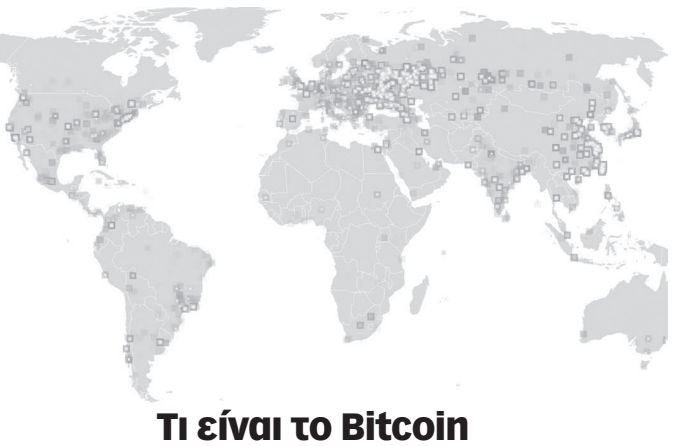
Η διαρροή αυτή που χρησιμοποιήθηκε από εγκληματίες του διαδικτύου έρχεται να προστεθεί σε μια σειρά αποκαλύψεων για τα προγράμματα παρακολούθησης της αμερικανικής κυβέρνησης. Σε tweet του ο'Εντουαρντ Σνόουντεν λίγο μετά την κυβερνοεπίθεση, επισημαίνει ότι «παρά τις προειδοποιήσεις, οι μυστικές υπηρεσίες συνεχίζουν να δημιουργούν επικίνδυνα εργαλεία που στοχεύουν στο δυτικό λογισμικό (σ.σ. Windows)» και διερωτάται «αν θα πρέπει το Κογκρέσο να ενημερωθεί από την NSA για άλλα παρόμοια τρωτά σημεία σε λογισμικά των νοσοκομείων της χώρας».

Όσο η παγκόσμια κοινότητα αντιμετώπιζε την απειλή του «WannaCry», το WikiLeaks δημοσίευσε δύο νέα κακόβουλα προγράμματα της CIA με στόχο πάλι τα Windows. Και τα δυο προγράμματα έχουν σχεδιαστεί για να παρακολουθούν και να αναφέρουν ενέργειες του χρήστη από τον μολυσμένο υπολογιστή. Η έκταση μάλιστα των αποκαλύψεων ήταν τέτοια που ανάγκασε τον πρόεδρο της Microsoft, Μπραντ Σμιθ, να καταδικάσει τις πρακτικές αυτές των μυστικών υπηρεσιών.

Οι ηλεκτρονικές επιθέσεις αλλάζουν μορφή

Μέχρι σήμερα οι απειλές από το χώρο του διαδικτύου περιορίζονταν στον ηλεκτρονικό κόσμο (υποκλοπές προσωπικών στοιχείων, χρηματικές απάτες κ.λπ.)'Ισως είναι η πρώτη φορά που αντιλαμβανόμαστε το πέρασμα του κυβερνοπολέμου στη σφαίρα της πραγματικής ζωής. Η απειλή του «WannaCry» κατέστησε σαφές τι έκτασης μπορεί

Η απειλή του «WannaCry» κατέστησε σαφές τι έκτασης μπορεί να είναι οι συνέπειες του κυβερνοπολέμου και πόσο ανυποψίαστο κόσμο είναι ικανή να επηρεάσει



Τι είναι το Bitcoin

Το Bitcoin είναι ένα ψηφιακό νόμισμα που ξεκίνησε στις αρχές της παγκόσμιας οικονομικής ύφεσης. Στόχος της δημιουργίας του είναι οι συναλλαγές χωρίς ενδιάμεσους παράγοντες (κυρίως αφορούσε τις τράπεζες).

Η κατοχή του νομίσματος κρυπτογραφείται για τον κάτοχό του, ενώ τα ίχνη των ψηφιακών συναλλαγών είναι αδύνατο να εντοπιστούν (αφού δεν υπάρχει κανένας ενδιάμεσος παράγοντας). Από τις αρχές του 2017 η αξία του νομίσματος σημειώνει άνοδο και σήμερα η αξία ενός Bitcoin κυμαίνεται γύρω στα 1.830 δολάρια! Να σημειώσουμε ότι στις 3 Μαρτίου η αξία του ξεπέρασε αυτή του χρυσού. (Βλέπε και φύλλο 346)