

”Χακάροντας” drones: ένας νέος κυβερνοκίνδυνος

/ [Πεμπτούσία](#)



Η βιομηχανία των drones αναπτύσσεται με ραγδαίους ρυθμούς, κι έρευνες δείχνουν πως οι πωλήσεις τους θα ξεπεράσουν τα 89 δις δολάρια τα επόμενα χρόνια. Η ραγδαία εξέλιξή τους όμως εγείρει και αρκετές ανησυχίες όσον αφορά την ασφάλειά τους και φυσικά την απειλή που θα μπορούσαν να αποτελέσουν για την ιδιωτικότητά μας.

Στο συνέδριο Virus Bulletin 2015, ο ερευνητής ασφαλείας της HP Security Research, Oleg Petrovsky έκανε λεπτομερή αναφορά στις μεθόδους που θα μπορούσαν να χρησιμοποιηθούν για το hack των μη επανδρωμένων εναέριων οχημάτων [unmanned aerial vehicles (UAVs)], γνωστών ως drones, τα οποία εκτελούν προγραμματισμένες διαδρομές.

Ο Oleg Petrovsky έκανε επίδειξη του πως θα μπορούσε κάποιος να hackάρει ένα drone στοχεύοντας τον ελεγκτή πτήσης του και ανέλυσε τους ελεγκτές διάφορων multi-rotor drones και ανακάλυψε αρκετές αδυναμίες που θα μπορούσαν να αξιοποιηθούν σε cyber attacks.

Παρά το γεγονός ότι υπάρχουν πολλά διαφορετικά μοντέλα drones διαθέσιμα στην αγορά, τα οποία όμως αποτελούνται κατά κύριο λόγο από τα ίδια βασικά μέρη, συμπεριλαμβανομένων των παρακάτω: κινητήρες, μπαταρίες, αισθητήρες, μια μονάδα GPS, ένα remote control radio receiver, electronic speed controllers (ESC), και τον ελεγκτή πτήσης.

Ο Petronsky κατά την έρευνά του επικεντρώθηκε στις επιθέσεις που έχουν ως στόχο τον ελεγκτή πτήσης, ο οποίος είναι ένα σύστημα που αποτελείται από διάφορους αισθητήρες και μια μονάδα επεξεργασίας. Η πλειοψηφία των drones χρησιμοποιεί τους ίδιους ελεγκτές πτήσης, όπως είναι τα ArduPilotMega (APM) και Pixhawk από την 3D Robotics, MultiWii, OpenPilot, και DJI Naza.

The screenshot displays the Mission Planner software interface. At the top, there are menu options: FLIGHT DATA, FLIGHT PLAN, INITIAL SETUP, CONFIG/TUNING, SIMULATION, TERMINAL, HELP, and DONATE. On the right, there are dropdown menus for COM3 and 115200, and a CONNECT button. The main area shows a satellite map with a yellow flight path connecting five waypoints (1-5) and a 'Home' location. A zoom slider is on the right. Below the map is a 'Waypoints' table with columns for Command, WP Radius, Loiter Radius, Default Alt, Absolute Alt, Verify Height, Lat, Long, Alt, Delete, Up, Down, Grad %, Dist, and AZ. The table contains five rows of waypoint data.

	Command	WP Radius	Loiter Radius	Default Alt	Absolute Alt	Verify Height	Lat	Long	Alt	Delete	Up	Down	Grad %	Dist	AZ
1	WAYPOINT	0	0	0	0		-35.0407928	117.8277898	100	X	🏠	🏠	95.7	104.5	1
2	WAYPOINT	0	0	0	0		-35.0406786	117.8260410	100	X	🏠	🏠	0.0	159.7	275
3	WAYPOINT	0	0	0	0		-35.0417239	117.8251612	100	X	🏠	🏠	0.0	141.2	215
4	WAYPOINT	0	0	0	0		-35.0428395	117.8259873	100	X	🏠	🏠	0.0	145.1	149
5	WAYPOINT	0	0	0	0		-35.0427165	117.8274572	100	X	🏠	🏠	0.0	134.5	84

Ένας πιθανός εισβολέας μπορεί να επικεντρώσει τις προσπάθειές του στο hacking αυτών των controllers, ώστε να καταφέρει να στοχεύσει σε ένα ευρύ φάσμα μοντέλων. Ο Petronsky χρησιμοποίησε για το test του ένα ArduPilotMega (APM) flight controller σε drone που έφτιαξε ο ίδιος και ένα Mission Planner, το οποίο είναι ένα ground station application.

Ο ερευνητής κατέγραψε με λεπτομέρειες μερικά σενάρια επίθεσης εναντίον drones με προγραμματισμένες διαδρομές χρησιμοποιώντας ground station software. Το ground station application είναι ένα κείμενο συστατικό της πτήσης ενός μη επανδρωμένου αεροσκάφους, αφού επιτρέπει την επικοινωνία με την κεραία του οχήματος και επιτρέπει στο χρήστη να το ελέγχει ασύρματα.

Ο [ερευνητής](#) τόνισε την έλλειψη authentication στα πρωτόκολλα που χρησιμοποιούνται για τον εξ αποστάσεως έλεγχο των μη επανδρωμένων αεροσκαφών, η οποία θα μπορούσε να αξιοποιηθεί από εισβολείς για να αποκτήσουν τον έλεγχο των οχημάτων.

Παρόλο τον μεγάλο αριθμό ερευνών που έχουν πραγματοποιηθεί για το hacking των drones, ο Petrovsky εξηγεί πως δεν υπάρχουν σημαντικές βελτιώσεις όσον αφορά την [ασφάλειά τους](#), και αυτό διότι δεν έχουν γίνει ακόμη real-world επιθέσεις σε εμπορικά μη επανδρωμένα εναέρια οχήματα.

Πηγή: secnews.gr