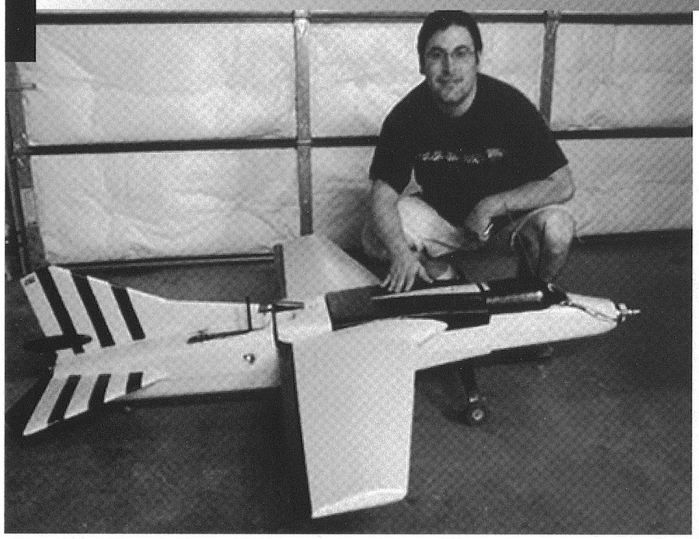
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2012)
Heft: 2

Artikel: WASP
Autor: Weck, Hervé de
DOI: https://doi.org/10.5169/seals-514653



WASP - ou le drône à l'ère du *do it yourself*.

News

WASP

Col Hervé de Weck

Ancien rédacteur en chef, RMS

Non, il s'agit point d'un White Anglo-Saxon Protestant à prix cassé mais duWireless Aerial Surveillance Platform, un ingénieux « drone e-spion » bricolé par deux professionnels de la cyber-sécurité et passionnés d'aéromaquettisme.

Auparavant, Richard Perkins et Mike Tassey exercèrent dans divers départements TI/télécoms de l'US Air Force et devinrent consultants en cybersécurité auprès du Pentagone et de plusieurs firmes militech. Peu à peu, ces deux passionnés d'aéromaquettisme rêvèrent d'un petit engin volant dédié à l'interception et au piratage des communications. En 2009, ils s'offrirent un drone-cible FDM-117B (utilisé dans les années 80 pour les entraînements de tir de l'US Air Force) et travaillèrent d'arrache-pied dans leur garage.

u fut remplacé par un moteur électrique moins bruyant alimenté par deux batteries 22,2 volts de lithium polymère (LiPo) lui permettant de voler pendant une demi-heure jusqu'à 22 000 pieds d'altitude. L'équipement interne céda la place à une dizaine d'antennes radio, à un disque USB de stockage 32 Go, à un périphérique universel de radio logiciel (connu sous l'acronyme USRP) et à un dongle 4 Go connectant le WASP au Wi-Fi, au Bluetooth et aux réseaux de téléphonie 2G/3G. Une caméra HD fut également installée près du nez de l'appareil.

Pour couronner le tout, le Wireless Aerial Surveillance Platform (ou VESPIDen latin) intègre la très populaire application linuxienne BackTrack, connue par les administrateurs réseaux et par les RSSI pour sa remarquable palette de fonctions : cartographie réseau, identification de vulnérabilité cryptographique/physique, test de pénétration, escalade de privilèges, maintien d'accès/couverture de traces, analyse de réseau sans fil, analyse de VOIP et de téléphonie, médecine digitale, développement et ingénierie inversée, etc.

Ainsi, le WASP peut se connecter à une antenne-relais de téléphonie mobile et/ou simuler son fonctionnement afin de leurrer les terminaux environnants, d'intercepter leurs communications texte/voix (en mode standard/crypté) puis de rediriger celles-ci vers le serveur de Perkins-Tassey au sol. En outre, le drone e-spion peut suivre une route préprogrammée et orbiter au-dessus d'une zone à la recherche de vulnérabilités réseaux tel un véritable drone ISR, son opérateur intervenant uniquement lors du décollage et de l'atterrissage.
À mi-parcours, Perkins et Tassey présentèrent le WASP aux conférences Black Hat et Defcon à l'été 2010 afin de démontrer aux milieux cyber-sécuritaires à quel point les particuliers, les entreprises et les administrations sont vulnérables (même dans un lieu isolé) face à une technologie espionne à la fois artisanale et bon marché. En effet, le WASP n'a nécessité que 6500 dollars et deux années de développement. L'ère de la prolifération robotique commencera au-dessus de chez vous...
Le site Rabbit-Hole fournit les multiples détails du WASP et quelques précieuses indications Do It Yourself au technoïde sournois que vous êtes. Suggestion à 128 bits : comment combiner du hacking volant avec du trucage wi-fi ?

http://www.youtube.com/watch?v=AdrUpmsyMZA&feature=player_embedded